IJSSAR International Journal of Social Sciences and Academic Research

www.ijssar.net ISSN: 2510-9782

Original Article

Received/Accepted Dates

13.03.2026/25.04.2026

DOI:10.52096/issar.03.01.02

Artificial Intelligence Usage: The Problem Of Personal Data Protectıon And Legal Liability

Assoc. Prof. Dr. Fikret ERKAN

Fikreterkan@hotmail.com, ORCID: 0009-0004-9462-7572

Original Article

Subject:Artificial Intelligence

Article Citation Information

Erkan, F. (2026). **Artificial Intelligence Usage: The Problem Of Personal Data Protectıon And Legal Liability**. International Journal of Social Sciences and Academic Research (IJSSAR), *(e-ISSN:* **2510-9782** *)* Vol:3, Issue:1; s. 27-101.

www.ijssar.net

DOI: **10.52096/issar.03.01.02**

Gönderim: 13.03.2026

Kabul: 25.04.2026

In[IJSSAR International Journal of Social Sciences and Academic Research]

Abstract

This Study Examines The İmpact Of Artificial İntelligence (AI) On The Protection Of Personal Data And The Legal Liability İssues Arising İn This Context From A Multi-Layered And Comparative Perspective. The Data-Driven Nature Of AI Systems—Characterized By Big Data Analytics, Algorithmic İnference Processes, And Transnational Operations—Renders Traditional Approaches To Data Protection And Liability Law İncreasingly İnadequate. Within This Framework, The Study First Analyzes The Concept Of Personal Data İn The Context Of The Legal Systems Of The European Union, The Council Of Europe, And The United Nations, Demonstrating That This Concept Has Evolved From A Static Legal Category İnto A Dynamic And Relational Construct.

Subsequently, The Study Explores The Relationship Between Data-Driven Decision-Making Processes Of AI Systems And Legal Liability, Concluding That Liability İs Evolving From A Classical Act-Based Model Toward A Data-Driven And Multi-Actor Structure. The Fact That AI-Related Harms Often Arise Not From A Single İdentifiable Act, But From Complex İnteractions Among Datasets, Algorithms, And The Actors Who Develop, Provide, And Use These Systems, Leads To The Emergence Of New Forms Of Liability.

The Study Further Conducts A Comparative Analysis Of The Legal Systems Of The European Union, The Council Of Europe, The United States, And China, Revealing The Absence Of A Globally Uniform Regulatory Framework For AI Liability. Although Each System Exhibits Certain Strengths, Their Fragmented And İnconsistent Structures Remain İnsufficient For Effectively Regulating Harms Arising From Transnational AI Applications.

Building On These Findings, The Study Proposes The **"Global Artificial Intelligence Liability System (G-AILS)"** Model As A Contribution To The Literature. This Model Offers A Comprehensive Legal Architecture Consisting Of Global Normative Principles, Multi-Actor Liability Allocation, Specialized Judicial Oversight Mechanisms, And Effective Compliance And Enforcement Structures. The Most Significant İnnovation Of The Proposed Model Lies İn Extending Liability Beyond İndividual Actors To İnclude States And Global Governance Structures, Thereby Redefining Liability Law Within A Systemic Framework.

In Conclusion, The Study Argues That İn The Age Of Artificial İntelligence, Legal Liability Must Transcend İndividual And National Boundaries, Evolving İnto A Global,

Data-Driven, And Multi-Actor Structure, And Proposes A New Paradigm Of İnternational Law Accordingly.

ijssareditor@gmail.com

Keywords: Concept Of Personal Data; Artificial Intelligence; Data Protection And Global Legal Transformation; AI Law; Relationship Between AI Liability And The Concept Of Data; Liability Regimes İn AI Systems (European Union, Council Of Europe, United States, And China); International Data Protection Law; GDPR; AI Act (Regulation (EU) 2024/1689 On Artificial Intelligence); Global Artificial Intelligence Liability System (G-AILS); International AI Court.

INTRODUCTION

The Rapid Development Of Artificial İntelligence Technologies Has Led To The Widespread Adoption Of Data-Driven Systems, Rendering The Protection Of Personal Data More Complex And Fragile. In Particular, The İncreasing Use Of AI İn Sectors İnvolving Sensitive Data—Such As Law, Healthcare, Banking, And Land Registry Systems—Has Generated New And Multi-Layered Risks İn Terms Of Data Security, Privacy, And Liability Regimes. However, The İssue Extends Beyond The Mere İncrease İn Data Breaches; İt Reflects A Deeper Structural Transformation. Indeed, The Core Problem Today İs That, Despite The Existence Of National And İnternational Data Protection Regulations, These Normative Frameworks Are Becoming İncreasingly İnadequate İn Addressing The Novel Forms Of Data Processing Generated By AI Technologies. In Other Words, AI Systems Are Surpassing The Limits Of Existing Legal Regulations And Reopening Fundamental Debates Within Data Protection Law.

In This Context, Even Comprehensive Regulatory Frameworks Such As The General Data Protection Regulation (GDPR) May Prove İnsufficient When Confronted With Big Data, Algorithmic İnference, And Automated Decision-Making Processes. AI Systems Not Only Process Existing Data But Also Generate New, Often Sensitive İnformation From İndirect Data Sources, Thereby Creating A New Domain Of Risk That Exceeds The Traditional Boundaries Of Data Protection Law. Accordingly, The Problem İs Not The Absence Of Legal Norms, But Rather The Functional Limitations Of Existing Norms İn The Face Of Technological Developments.

This Study Examines The İmpact Of AI Usage On The Protection Of Personal Data From A Multidimensional Perspective. By İdentifying The Limitations Of National And İnternational Regulations İn Addressing AI-Related Challenges, İt Analyzes—Through A Comparative Legal Method—How Liability Regimes Should Be Restructured. In Doing So, The Study Not Only Evaluates Existing Regulatory Frameworks But Also Aims To Provide A Theoretical And Normative Framework For Rethinking Data Protection Law İn The Age Of Artificial İntelligence.

I. PERSONAL DATA AND APPROACHES IN THE EUROPEAN UNION, THE COUNCIL OF EUROPE, AND THE UNITED NATIONS SYSTEMS

1. The Concept Of Personal Data

The Concept Of Personal Data Constitutes A Central Notion Forming The Foundation Of Modern Data Protection Law. Both National And İnternational Legal Systems Establish Regulatory Frameworks That Define The Scope Of This Concept And Govern The Processing Of Data[1].

The Definition Of Personal Data İs Directly Linked To Fundamental Rights. Any Narrowing Of This Definition İnevitably Results İn A Restriction Of Those Rights. For This Reason, The Concept Of Personal Data Has Evolved From A Purely Technical İssue İnto A Constitutional Matter, And Has Accordingly Been İncorporated İnto İnternational Legal İnstruments. In This Context, The Concept Of Personal Data İs Examined Below Within The Frameworks Of The European Union, The Council Of Europe, And The United Nations.

[1] Under European Union law, *processing* is defined as any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means. This includes, inter alia, collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction (General Data Protection Regulation, Art. 4(2)).

1.1. The Concept Of Personal Data İn European Union Law

Within European Union Law, The General Data Protection Regulation (GDPR), Adopted İn 2016 And Entering İnto Force İn 2018, Constitutes A Binding Legal Framework Governing Personal Data[2]. Article 4(1) Of The GDPR Defines Personal Data As:

"Any İnformation Relating To An İdentified Or İdentifiable Natural Person."

According To This Definition, Once An İndividual İs İdentified (For Example, When Their Name İs Known), All Data Collected İn Relation To That Person Qualifies As Personal Data. The Same Applies Where The İndividual Has Not Yet Been İdentified But İs *İdentifiable*. This Means That A Person Can Be İdentified Either Directly Or İndirectly. Accordingly, The Definition İs İnterpreted Broadly So As To Encompass Not Only Directly İdentifying Data, But Also Any Data That Enables The İdentification Of An İndividual İndirectly.

In This Context, The Concept Of Personal Data Covers A Wide Spectrum, İncluding[3]:

- Directly İdentifying Data Such As Name, Surname, And İdentification Number;
- Location Data, IP Addresses, And Online İdentifiers;
- Health Records, Financial İnformation, And Social Relations.

Indirect İdentification, On The Other Hand, Refers To Situations Where Data Cannot Be Linked To An İndividual On İts Own, But Can Lead To İdentification When Combined With Other Available İnformation. Such Data Often Relates To Characteristics Of The İndividual's

[2] Although the GDPR constitutes the most comprehensive and binding instrument within European Union data protection law, the legal nature of the concept of personal data cannot be fully explained solely by reference to this regulation. This is because the right to data protection is, in essence, a constitutional right grounded in Article 8 of the Charter of Fundamental Rights of the European Union and in the provisions of the Treaty on the Functioning of the European Union. The GDPR represents the concretised and operationalised expression of this fundamental right. In this context, while the GDPR is a binding and directly applicable legal instrument, it does not constitute the primary normative source determining the scope of the concept of personal data. Rather, the concept functions as a **constitutional threshold**, delineating the scope of application of the fundamental right to data protection. Accordingly, any modification to the definition of personal data cannot be regarded merely as a technical regulatory adjustment; instead, it amounts to a **constitutional intervention** that directly affects the scope and substance of the right to data protection.

[33] Data relating to deceased persons, organisations (legal entities), or animals is not considered personal data under the GDPR and is therefore excluded from its scope. Nonetheless, such data may be regulated under other applicable legal regimes. See Universiteit Gent, *What is personal data?*, available at: https://onderzoektips.ugent.be/en/tips/00001781/ (accessed 01/04/2026)

Physical, Physiological, Genetic, Psychological, Economic, Cultural, Or Social İdentity. Examples İnclude Postal Codes, Age, Gender, Response Times To Specific Tasks, Brain Activity (E.G., EEG), Blood Glucose Levels, Personality Traits, And Heart Rate.

Accordingly, Data Qualifies As Personal Data Where İt[4]:

- Directly Leads To The İdentification Of A Person;
- Enables İdentification When Combined With Other Data;
- İs Linked To An İdentifiable İndividual, Even İf İt Does Not İndependently Reveal İdentity.

1.1.1. Types And Classification Of Personal Data

Personal Data İs Categorized Based On İts Nature And İts Role İn İdentifying An İndividual. This Classification İs Of Critical İmportance İn Determining The Level Of Protection To Be Applied Under Data Protection Law.

First, **Direct İdentifiers** Refer To Data That, On Their Own, Clearly Reveal The İdentity Of An İndividual. This İncludes İnformation Such As Name, Surname, İdentification Number, And Photographs, Which Can İdentify A Person Without Requiring Additional Data.

By Contrast, **İndirect İdentifiers** Do Not İndependently İdentify An İndividual But Render A Person İdentifiable When Combined With Other Data. Age, Gender, Location Data, And Behavioral Data Fall Within This Category. In The Digital Environment, The İncreasing Possibility Of Re-İdentification Through Data Aggregation Has Significantly Enhanced The İmportance Of İndirect İdentifiers.

In Addition, Data Protection Law Recognizes A Distinct Category Of **Special Categories Of Personal Data (Sensitive Data)**, Which Carry A Higher Risk For Fundamental Rights And Freedoms. Pursuant To Article 9 Of The GDPR, This Category İncludes:

- Racial Or Ethnic Origin;
- Political Opinions;
- Religious Or Philosophical Beliefs;
- Trade Union Membership;

[4] https://onderzoektips.ugent.be/en/tips/00001781/

- Genetic And Biometric Data;
- Health Data;
- Data Concerning A Person's Sex Life Or Sexual Orientation.

Due To Their High-Risk Nature, Such Data Are Subject To Stricter Protection Regimes And Are, As A Rule, Prohibited From Processing, Except Under Explicit Consent Or Narrowly Defined Legal Exceptions.

This Approach Demonstrates That Data Protection Law Has Evolved From A Purely Categorical Framework İnto A **Risk-Based Structure** That Takes İnto Account The İmpact Of Data On The İndividual.

1.1.2. Anonymisation And Pseudonymisation

One Of The Most Critical Distinctions İn Data Protection Law Concerns The Difference Between Anonymisation And Pseudonymisation. This Distinction İs Essential İn Determining Both The Legal Nature Of The Data And The Applicable Regulatory Framework.

Pseudonymised Data Refers To Data Where The Direct Link Between The Data And The Data Subject Has Been Removed, Yet Re-İdentification Remains Possible Through The Use Of Additional İnformation. In Such Cases, The Data Does Not Lose İts Personal Nature And Continues To Fall Within The Scope Of The GDPR. Consequently, All Processing Activities İnvolving Such Data Remain Subject To Data Protection Law.

By Contrast, **Anonymised Data** Refers To Data Where The İdentity Of The Data Subject Has Been İrreversibly Removed, And Re-İdentification İs No Longer Possible Through Any Reasonable Means. In Such Cases, The Data Ceases To Qualify As Personal Data And Falls Outside The Scope Of The GDPR.

However, İt İs Crucial To Note That The Anonymisation Process İtself Constitutes A Data Processing Activity. In Other Words, Until Anonymisation İs Completed, The Data Retains İts Status As Personal Data And Remains Subject To GDPR Provisions Throughout The Process[5].

[5] This distinction is of particular significance in the context of large datasets used in artificial intelligence systems. AI algorithms are often capable of re-identifying individuals even from data assumed to be anonymised and of generating sensitive inferences from indirect data. This development necessitates a reconsideration of the concept of anonymity within data protection law.

1.1.3. The Approach Of The Court Of Justice Of The European Union (CJEU)

The Established Case Law Of The Court Of Justice Of The European Union (CJEU) Confirms This Broad İnterpretation Of Personal Data. The Court Has Consistently Held That Personal Data İs Not Limited To Directly İdentifying İnformation, But Also İncludes Any Data That Enables The İndirect İdentification Of An İndividual.

In This Regard, İn **Breyer V Bundesrepublik Deutschland**[6], The Court Examined The Legal Nature Of Dynamic IP Addresses. The Dispute Concerned Whether Such IP Addresses Could Be Considered Personal Data Where İdentification Of The İndividual Was Possible Through A Third Party Possessing Additional İnformation. The Court Held That Even Where The Data Controller Cannot Directly İdentify The İndividual, The Data Qualifies As Personal Data İf İdentification İs Possible By Reasonable Means Through Third Parties.

In İts Reasoning, The Court Emphasized The Criterion Of "Means Reasonably Likely To Be Used," Concluding That Even İndirect Access To Additional İnformation May Suffice For Data To Retain İts Personal Character. This Approach Reflects A Functional And Contextual İnterpretation Of Personal Data.

Similarly, İn **Google Spain SL V AEPD And Mario Costeja González**[7], The Court Examined Whether Search Engine Activities Fall Within The Scope Of Data Protection Law. The Case Concerned A Request To Remove Outdated Financial İnformation From Search Engine Results Under The "Right To Be Forgotten."

The CJEU Held That The Activities Of Search Engine Operators—İncluding İndexing, Storing, Organizing, And Making İnformation Accessible—Constitute "Processing Of Personal Data." Furthermore, The Court Recognized The Search Engine Provider As A **Data Controller**, Given İts Decisive İnfluence Over Such Processing Activities.

One Of The Most Significant Aspects Of This Judgment İs İts Recognition That Personal Data İs Not Limited To Raw İnformation, But Also İncludes The Manner İn Which Data İs

[6] Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* EU:C:2016:779 (19 October 2016).
[7] Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* EU:C:2014:317 (13 May 2014)

Processed, Presented, And Made Accessible. The Court Emphasized That The Creation And Accessibility Of An İndividual's Digital Profile Fall Within The Scope Of Data Protection Law.

Taken Together, These Decisions Demonstrate That The CJEU Adopts An Approach To Personal Data That İs:

- Functional Rather Than Purely Technical;
- Dynamic Rather Than Static;
- Broad Rather Than Restrictive.

These Rulings Are Particularly Significant İn The Context Of AI Systems, Where İndirect Data And İnference Processes Play A Central Role, And They Confirm The Extensive Scope Of Data Protection Law.

When The GDPR And CJEU Case Law Are Considered Together, İt Becomes Clear That The Concept Of Personal Data İs Far More Than A Mere Technical Definition Within EU Law. Rather, İt Performs A Structural Function By Delineating Not Only The Scope Of Data Protection Law But Also The Substantive Boundaries Of The Right To Data Protection As Guaranteed Under Article 8 Of The Charter Of Fundamental Rights Of The European Union And The Broader Data Protection Regime Under The Treaty On The Functioning Of The European Union.

Accordingly, The Definition Of Personal Data Constitutes Not Merely A Normative Element, But A **"Constitutional Threshold"** Determining The Applicability Of A Fundamental Right. Over Time, This Concept Has Evolved From A Regulatory Term İnto A **Quasi-Constitutional Construct**, Directly Shaping Both The Scope Of Data Protection And The Broader System Of Fundamental Rights.

Therefore, Any Restrictive İnterpretation Or Modification Of This Definition Should Not Be Regarded As A Purely Technical Adjustment, But Rather As An İntervention İnto The Scope Of Fundamental Rights Themselves.

1.2. The Concept Of Personal Data İn The Council Of Europe Legal Framework

Within The Legal System Of The Council Of Europe, The Concept Of Personal Data İs Approached Not Merely As A Technical İssue Of Data Protection—As İs More Characteristic

Of European Union Law—But Rather As A Human Rights–Based Concept Grounded Primarily İn The Right To Respect For Private Life. In This Regard, The Normative Foundation Of The Concept İs Rooted İn Article 8 Of The European Convention On Human Rights (ECHR).

However, The Council Of Europe's Approach To Data Protection İs Not Limited To This Foundational Provision. When Considered Together With Convention 108 And İts Modernized Version (Convention 108+), Relevant Recommendations And Guidance Documents, And The Established Case Law Of The European Court Of Human Rights (Ecthr), A Comprehensive And Multi-Layered Framework Emerges. This Normative And Judicial Architecture Clearly Demonstrates That The Council Of Europe Conceptualizes Personal Data Not As A Narrow Technical Category, But As A Dynamic, Broadly İnterpretable Legal Construct Directly Linked To Human Rights.

1.2.1. Article 8 ECHR And The Human Rights Foundation Of Personal Data

According To Article 8 Of The ECHR:

"Everyone Has The Right To Respect For His Private And Family Life, His Home And His Correspondence."

Although The Concept Of Personal Data İs Not Explicitly Defined İn This Provision, The European Court Of Human Rights Has Expanded İts Scope Through İts Jurisprudence, İnterpreting Data Processing Activities Within The Framework Of The Right To Respect For Private Life.

In This Context, The Ecthr:

- Does Not Limit The Concept Of Personal Data To Directly İdentifying İnformation;
- İnterprets İt Broadly To İnclude All İnformation Relating To An İndividual's İdentity, Behavior, And Private Life.

As A Result, The Concept Of Personal Data Acquires A **Functional And Human-Centered Meaning** Within The Council Of Europe System.

1.2.2. Ecthr Jurisprudence: Expansive Interpretation Of Personal Data

The European Court Of Human Rights Has Developed The Concept Of Personal Data Not Through A Formal Definition, But Through Case Law Based On Concrete Disputes. Through İts İnterpretation Of Article 8 ECHR, The Court Has Expanded The Scope Of Personal Data And Brought Data Processing Activities Within The Ambit Of The Right To Private Life. This Approach Reveals That Personal Data İs Not Merely A Technical Category But A Dynamic Concept İntrinsically Linked To Human Rights.

Key Judgments Of The Ecthr İnclude:

- **S. And Marper V United Kingdom**
  The Court Held That The İndefinite Retention Of DNA And Fingerprint Data Constituted A Violation Of Article 8 ECHR. It Emphasized The Highly Sensitive Nature Of Biometric Data And Concluded That Such Retention Amounted To A Serious İnterference With Private Life.
- **Amann V Switzerland**
  The Court Recognized That The Mere Collection And Storage Of Personal Data, Even Without Further Use, Constitutes An İnterference With Private Life.
- **Rotaru V Romania**
  The Court Ruled That The Collection And Retention Of Personal İnformation By State Authorities Must Comply With Legality, Foreseeability, And Proportionality Requirements.
- **Uzun V Germany**
  The Court Held That GPS-Based Tracking And The Collection Of Location Data Fall Within The Scope Of Private Life And Constitute An İnterference Under Article 8.

Taken Together, These Decisions Demonstrate That The Ecthr:

- İnterprets Personal Data Broadly And Dynamically;
- Subjects All Stages Of Data Processing (Collection, Storage, Analysis) To Legal Scrutiny;
- Continuously Expands The Scope Of The Concept İn Line With Technological Developments.

Accordingly, Ecthr Jurisprudence Transforms Personal Data From A Narrow Technical Category İnto A **Core Element Of The Right To Respect For Private Life**.

1.2.3. Council Of Europe Convention: Convention 108 And Its Modernization

The Most Fundamental And Binding İnternational İnstrument Of The Council Of Europe İn The Field Of Data Protection İs Convention 108. Adopted İn 1981, İt İs The First İnternational Legal İnstrument Aimed At Protecting İndividuals Against The Automatic Processing Of Personal Data. The Convention Establishes The Core Concepts And Principles Of Data Protection Law And Provides A Common Normative Framework For İts Member States.

Within This Framework, Personal Data İs Defined As "Any İnformation Relating To An İdentified Or İdentifiable İndividual." This Definition Encompasses Both Directly İdentifying Data And Data That Allows İndirect İdentification, Thereby Reflecting A Broad And İnclusive Understanding Of Personal Data.

With The Acceleration Of Technological Developments And Digitalization, The Convention Was Modernized İn 2018 As Convention 108+. This Modernization Aimed To Align Data Protection Law With Emerging Technological Risks. The Revised Framework:

- Strengthened Principles Of Transparency And Accountability;
- İntroduced Enhanced Rules On Cross-Border Data Flows;
- Explicitly İncorporated Automated Data Processing Systems And Algorithmic Decision-Making;
- Expanded İndividual Rights, Particularly The Rights Of Access And Objection.

One Of The Most Significant Contributions Of Convention 108+ Lies İn Extending The Scope Of Data Protection Law To Encompass Artificial İntelligence, Big Data Analytics, And Automated Decision-Making Processes. In This Respect, The Modernization Demonstrates That The Council Of Europe Perceives Data Protection Not As A Static Regulatory Domain, But As A **Dynamic Normative System Adaptable To Technological Change**.

1.2.4. Council Of Europe Recommendations And Guidelines

In Addition To Binding Conventions, The Council Of Europe Expands The Scope Of Data Protection Law Through Various Recommendations And Guidance Documents. Although

These İnstruments Are Not Legally Binding, They Serve An İmportant Guiding Function For Member States And Play A Significant Role İn The Development Of Data Protection Law.

In This Context, The Council Of Europe Has Developed Specific Recommendations İn High-Risk Areas Such As:

- Processing Of Law Enforcement And Police Data;
- Protection Of Health Data;
- Biometric And Genetic Data;
- Artificial İntelligence Systems And Algorithmic Decision-Making.

Within These İnstruments, The Concept Of Personal Data İs Not Treated As A Fixed And Narrowly Defined Category. Instead, İt İs Understood As A Legal Concept That:

- Expands Contextually (*Contextual Expansion*);
- İs Assessed Through A Risk-Based Approach;
- Adapts To Technological Developments.

This Perspective Highlights That Data Protection Law Should Focus Not Only On The Nature Of Data İtself, But Also On How Data İs Processed, The Purposes For Which İt İs Used, And The Risks İt May Generate.

In Particular, Council Of Europe Documents On Artificial İntelligence And Automated Decision-Making Emphasize That Personal Data İs Not Limited To Raw Data; Rather, **İnferences Derived From Data** May Also Significantly Affect İndividuals' Rights And Freedoms. This Approach Extends The Scope Of Data Protection Law And Promotes A Preventive, Risk-Oriented Governance Model.

General Assessment

Within This Comprehensive Framework, The Concept Of Personal Data Emerges:

- Not As A Static Category Based Solely On Formal Definitions;
- But As A Legal Construct Shaped By Strong Judicial İnterpretation;
- Grounded İn Human Rights And Expanding Contextually.

The Council Of Europe's Approach Can Be Summarized Around Three Core Characteristics:

1. The Concept Of Personal Data Has Acquired A Dynamic Normative Content That Evolves Continuously Through Ecthr Jurisprudence And Adapts To Technological Transformations.
2. It İs Directly Linked To The Right To Respect For Private Life, Thereby Elevating Data Protection From A Technical Field To A Fundamental Human Rights Dimension.
3. The System Adopts A Robust Protective Stance Vis-À-Vis State Authorities, Subjecting Data Processing Activities To Strict Scrutiny Under The Principles Of Legality, Necessity, And Proportionality.

In This Sense, Within The Council Of Europe Framework, Personal Data İs Not Merely A Technical Element Of Data Protection Law, But A Legal Value İntrinsically Connected To Human Dignity, Privacy, And İndividual Autonomy, Forming An İntegral Component Of The Right To Private Life.

1.3. The Concept Of Personal Data İn The United Nations Legal Framework

Within The Legal Framework Of The United Nations (UN), The Concept Of Personal Data İs Not Explicitly Defined Within A Single Binding İnstrument, Unlike İn European Union Law. However, When The Data Protection Principles, Human Rights İnstruments, And İnstitutional Frameworks Developed Within The UN System Are Considered Together, İt Becomes Evident That The Concept Of Personal Data İs Approached Through A Broad, Contextual, And Human Rights–Based Perspective. In This Regard, Within The UN System, The Definition Of Personal Data Evolves Not As A Rigid Legal Category, But As A Flexible, Human Rights–Oriented, And Context-Dependent Concept.

Accordingly, The UN Approach Reflects Not A Codified Normative Framework, But Rather A Principle-Based And Multi-Layered Structure.

1.3.1. UN Data Protection Principles And Definition

The Most Explicit Definition Of Personal Data Within The UN System İs Found İn The Document Titled *"**Personal Data Protection And Privacy Principles**[8]"* (11 October 2018), Adopted By The United Nations System Chief Executives Board For Coordination.

[8] https://unsceb.org/sites/default/files/imported_files/UN-Principles-on-Personal-Data-Protection-Privacy-2018_0.pdf

In This Document, Personal Data İs Defined As:

"Any İnformation Relating To An İdentified Or İdentifiable Natural Person."

This Definition:

- Encompasses Directly İdentifying Data;
- İncludes Data Through Which İdentification Can Be Made İndirectly;

And İs Therefore Largely Aligned İn Scope With The GDPR Definition.

The Document Further Sets Out The Fundamental Principles Of Data Protection As Follows:

- Lawfulness And Fairness;
- Purpose Limitation;
- Data Minimization;
- Accuracy;
- Security.

These Principles Demonstrate That, Within The UN System, The Concept Of Personal Data İs Not Merely A Definitional Element But A Dynamic Concept That Derives Meaning Within A Broader Normative Framework Of Principles.

1.3.2. Human Rights Foundation: The Right To Privacy

In UN Law, The Concept Of Personal Data İs Not Treated As An Autonomous Legal Field, But Rather İs Directly Situated Within The Framework Of İnternational Human Rights Law, Particularly İn Relation To The Right To Privacy. In This Context, The Primary Normative Foundation İs Article 17 Of The International Covenant On Civil And Political Rights (ICCPR).

According To This Provision[9]:

"No One Shall Be Subjected To Arbitrary Or Unlawful İnterference With His Privacy, Family, Home Or Correspondence."

[9] According to this provision, no one shall be subjected to arbitrary or unlawful interference with their private life, family, home, or correspondence. This rule constitutes the normative foundation of the right to data protection and plays a central role in determining the scope of the concept of personal data.

This Provision Constitutes The Core Basis Of Data Protection Within The UN System. The Human Rights Committee, İn İts General Comment No. 16 (1988), İnterpreted This Provision By Emphasizing That[10]:

- Data Storage,
- Data Processing,
- And Access To Data

Should All Be Considered Within The Scope Of The Right To Privacy.

Although This İnterpretation Does Not Provide An Explicit Definition Of Personal Data, İt Adopts An Expansive Approach By Framing Data Processing Activities As Potential İnterferences With Privacy, Thereby Broadening The Scope Of The Concept.

1.3.3. UN Human Rights Council And Digital Privacy

The United Nations Human Rights Council's Resolutions On *"The Right To Privacy İn The Digital Age"* (Resolutions 2013/24, 2014/22, 2018/7, And 2021/12) Have Played A Significant Role İn The Global Development Of Data Protection Law.

In These Resolutions, The Following Practices Are İdentified As Posing Serious Risks To Human Rights:

- Mass Data Collection;
- Surveillance Technologies;
- Algorithmic Data Analysis.

Although These Documents Do Not Explicitly Define Personal Data, They Adopt A Broad İnterpretation Of Data Processing Activities, Effectively Contributing To The Development Of A Comprehensive Data Protection Understanding At The Global Level.

This Approach Demonstrates That The Concept Of Personal Data İs Not Fixed Or Purely Technical, But Rather Evolves Dynamically İn Response To Technological Developments.

[10] BM İnsan Hakları Komitesi **General Comment No. 16 (1988).**

1.3.4. Judicial Perspectives And International Law Dimension

Although The UN System Does Not İnclude A Directly Binding İnternational Judicial Decision Specifically Addressing The Concept Of Personal Data, Certain Judicial Approaches Suggest That Data And İnformation Processing Activities May Give Rise To İnternational Responsibility.

In This Context, İn The Case Of **Certain Activities Carried Out By Nicaragua İn The Border Area**[11], The International Court Of Justice (ICJ), While Not Directly Addressing Data Protection, İndicated That The Use Of İnformation And Data May Be Assessed Within The Framework Of State Responsibility.

This Perspective İs Significant İn Demonstrating That Data Processing Activities May Give Rise Not Only To İndividual Liability But Also To İnternational Responsibility At The State Level.

In Conclusion, Within The UN System, The Concept Of Personal Data:

- İs Not Codified Within A Single Binding Norm;
- İs Structured As A Principle-Based And Flexible Legal Framework;
- İs Directly Linked To Human Rights.

Accordingly, The UN Approach Conceptualizes Personal Data Not As A Narrowly Defined Technical Category, But As A Legal Construct Embedded Within The Protection Of Privacy And Human Dignity, And Evolving İn Response To Global Technological Developments.

1.4. Comparative Analysis Of The Concept Of Personal Data İn The European Union, The United Nations, And The Council Of Europe Systems

The Table Below Presents A Comparative Overview Of How The Concept Of Personal Data İs Approached Within The Legal Frameworks Of The European Union, The United Nations, And The Council Of Europe/European Court Of Human Rights Systems.

[11] International Court of Justice (ICJ) 16 Aralık 2015 tarihli Certain Activities Carried Out by Nicaragua in the Border Area

This Comparative Analysis Clearly Reveals The Fundamental Differences İn How These Three Systems Conceptualize Personal Data.

European Union Approach: Within The European Union, The Concept Of Personal Data İs Defined Through A Clear, Codified, And Technically Structured Legal Norm. This Approach:

- Ensures A High Degree Of Legal Certainty;
- İs Supported By Strong Enforcement And Sanctioning Mechanisms.

However, İt May Encounter Limitations İn Terms Of Flexibility When Confronted With Rapid Technological Developments.

United Nations Approach: The United Nations System Approaches The Concept Of Personal Data Within A Framework That İs:

- Principle-Based;
- Flexible;
- Contextual.

The Principal Advantage Of This Approach Lies İn İts Capacity To Facilitate Global Harmonization. However, İts Lack Of Binding Force Constitutes A Significant Limitation.

Council Of Europe / Ecthr Approach: Within The Council Of Europe System, The European Court Of Human Rights Develops The Concept Of Personal Data:

- Not Through A Formal And Explicit Definition;
- But Through Case Law;
- And Within The Broader Framework Of Human Rights.

The Most Distinctive Strength Of This Approach Lies İn İts Direct Linkage Of The Concept Of Data To **Human Dignity And The Right To Respect For Private Life**.

In Conclusion, Although The Concept Of Personal Data İs Defined Through Different Methods Across Various Legal Systems, İt Consistently Revolves Around A Common Normative Core: İts Direct And İntrinsic Connection To Human Rights.

Table 1: Comparative Analysis Of The Concept Of Personal Data

Criterion	European Union (EU)	United Nations (UN)	Council of Europe / ECtHR
Primary Norm	General Data Protection Regulation (GDPR), Art. 4(1)	UN Personal Data Protection and Privacy Principles (2018)	European Convention on Human Rights (ECHR)
Nature of Definition	Explicit and codified	Principle-based	Case law–based
Definition	"Any information relating to an identified or identifiable natural person"	Same or similar formulation	No explicit definition; developed through jurisprudence
Regulatory Approach	Normative (rule-based)	Principle-based	Human rights–based
Scope	Broad and technical	Broad and flexible	Very broad and dynamic
Indirect Data	Explicitly covered	Covered	Broadly interpreted through case law
Sensitive Data	Explicitly regulated (Art. 9 GDPR)	Protected at the principle level	Strongly protected through jurisprudence
Approach to Anonymisation	Anonymous data falls outside scope	Contextual assessment	Risk of re-identification assessed in practice
Data Processing Approach	Regulated and systematic	Principle-based	Interference test (under Article 8 ECHR)

2. THE CONCEPT OF ARTIFICIAL INTELLIGENCE AND THE TRANSFORMATION OF THE CONCEPT OF DATA IN THE CONTEXT OF AI

2.1. The Concept Of Artificial Intelligence

Artificial İntelligence (AI), İn İts Broadest Sense, Refers To The Ability Of Computer Systems To Simulate Human-Like Cognitive Processes. Within This Scope, AI Emerges As A Technological Paradigm That Enables The Execution Of Functions Traditionally Associated With Human İntelligence—Such As Learning, Problem-Solving, Decision-Making, Language Comprehension, And Creative Content Generation—Through Machine-Based Systems (Erkan, 2025, P. 298).

The Concept Of Artificial İntelligence Was First İntroduced By John Mccarthy At The Dartmouth Conference İn 1956 (Russell & Norvig, 2010). While Early Developments Focused On Symbolic Logic-Based Systems, Contemporary AI İs Predominantly Shaped By Machine Learning And, İn Particular, Deep Learning Approaches (Erkan, 2026, Pp. 161–162)[12].

However, The Concept Of Artificial İntelligence İs Not Limited To A Purely Technical Definition; İt İs İncreasingly Addressed Within A Normative Framework İn İnternational Legal İnstruments. In This Context, Defining AI Systems İs Crucial Not Only For Understanding

[12] Artificial intelligence (AI) also encompasses subfields such as machine learning (ML) and deep learning (DL). Machine learning enables systems to learn from experience, whereas deep learning employs larger datasets and more complex neural network structures to achieve more advanced learning processes.

Their Functional Characteristics But Also For Assessing Their İmpact On İndividuals And Society.

2.1.1. Definition Of Artificial Intelligence İn International Law

One Of The Most Comprehensive Definitions Of Artificial İntelligence At The İnternational Level İs Found İn The *Framework Convention On Artificial Intelligence, Human Rights, Democracy And The Rule Of Law*[13], Adopted By The Council Of Europe. According To This Convention, An AI System İs Defined As:

"A Machine-Based System That, For Explicit Or İmplicit Objectives, Generates Outputs Such As Predictions, Content, Recommendations, Or Decisions İnfluencing Physical Or Virtual Environments, Based On The İnputs İt Receives."

Similarly, The European Union's AI Act (Regulation (EU) 2024/1689[14]) Adopts A More Technical And Functional Definition. According To The AI Act, An AI System İs:

"A Machine-Based System Designed To Operate With Varying Levels Of Autonomy, Capable Of Adapting After Deployment, And Generating Outputs Such As Predictions, Content, Recommendations Or Decisions That İnfluence Physical Or Virtual Environments Based On İnput Data."

When These Definitions Are Considered Together, The Core Characteristics Of AI Systems Can Be İdentified As Follows:

- Being Machine-Based Systems;
- Performing İnference From Data İnputs;
- Producing Outputs Such As Predictions, Recommendations, Or Decisions;
- İnfluencing Physical Or Digital Environments;

[13] The Convention was adopted by the Committee of Ministers of the Council of Europe on 17 May 2024 and was opened for signature on 5 September 2024 in Vilnius, Lithuania, during the Conference of Ministers of Justice of the Council of Europe.

[14] The EU Artificial Intelligence Act (Regulation (EU) 2024/1689) was published in the Official Journal of the European Union on 12 July 2024, becoming the first comprehensive horizontal legal framework for the regulation of AI systems across the EU. The Regulation will enter into force on 1 August 2024 in all 27 EU Member States, with most of its provisions becoming applicable from 2 August 2026. See the full text: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401689 (accessed 1 July 2025).

- İncorporating A Certain Degree Of Autonomy.

From This Perspective, Artificial İntelligence Should Not Be Regarded Merely As A Software Tool, But As A Set Of Autonomous Or Semi-Autonomous Systems Capable Of Generating Decisions.

2.1.2. Main Types Of Artificial Intelligence

AI Systems Can Generally Be Classified İnto Three Main Categories Based On Their Functional Capabilities:

(İ) Artificial Narrow Intelligence (ANI):
These Systems Perform Specific, Often Complex Tasks Such As Pattern Recognition Or Prediction[15]. They May Reach Or Even Exceed Human-Level Performance Within A Defined Domain (E.G., Voice Assistants Or Recommendation Systems), But Lack General Cognitive Ability.

(İi) Artificial General Intelligence (AGI):
AGI Refers To Systems Capable Of Learning And Problem-Solving Across Multiple Domains İn A Manner Comparable To Human İntelligence. These Systems Remain Largely Theoretical And Aim To Achieve Generalized Cognitive Capabilities.

(İii) Generative Artificial Intelligence (Genaı):
Genaı Systems Are Capable Of Producing New And Original Content—Such As Text, İmages, Or Audio—Through Algorithms Trained On Large Datasets. Using Deep Learning Techniques, These Systems Generate Meaningful And Often Creative Outputs. Typically, They Rely On Massive Datasets To Understand, Summarize, Generate, And Predict Content, Producing Outputs That Appear Novel And Realistic[16].

2.1.3. Technological Infrastructure Of Artificial Intelligence

[15] University of Notre Dame. (n.d.). *AI overview and definitions*. Notre Dame Learning. Retrieved June 27, 2025, from https://learning.nd.edu/resource-library/ai-overview-and-definitions/
[16] Notre Dame, *AI Overview and Definitions*.

Artificial İntelligence İs Built Upon A Complex Technological Ecosystem Composed Of Several Subfields. In Particular:

- **Machine Learning:** Enables Systems To Learn From Data.
- **Deep Learning:** Allows Complex Data Analysis Through Multi-Layered Neural Networks.
- **Natural Language Processing (NLP):** Facilitates The Understanding And Processing Of Human Language.
- **Computer Vision:** Enables The Analysis And İnterpretation Of Visual Data.

These Technological Components Highlight The İntrinsic Relationship Between AI Systems And Data, Reinforcing The Fundamentally Data-Driven Nature Of Artificial İntelligence.

2.2. The Transformation Of The Concept Of Data İn The Context Of Artificial Intelligence

The Development Of Artificial İntelligence Technologies Fundamentally Transforms The Place Of Personal Data Within The Classical Framework Of Data Protection Law. Traditionally, Personal Data Has Been Understood Within A Relatively Limited Scope, Focusing On The Collection And Processing Of İnformation Directly Or İndirectly Related To An İndividual.

However, AI Systems Not Only Process Existing Data But Also Possess The Capacity To Generate New İnformation—Often Of A More Sensitive Nature—From That Data. This Development Transforms Data From A Static Category İnto A Dynamic, Generative, And Predictive Construct.

2.2.1. From Data To Inference

Traditional Data Protection Approaches Conceptualize Data Processing As Limited To Data Collection, Storage, And Use. In Contrast, AI Systems—Particularly Those Based On Machine Learning—Are Capable Of:

- Establishing Relationships Between Datasets;
- Generating New İnformation About İndividuals;
- Predicting Future Behavior.

This Gives Rise To What İs Commonly Referred To As The **"İnference Problem."**

AI Systems Can İnfer Highly Sensitive İnformation—Such As Health Conditions, Political Opinions, Economic Behavior, And Psychological Profiles—From İndirect Data Without Relying On Explicit Personal Data. This Challenges The Fundamental Assumption Of Traditional Data Protection Law And Supports The Argument That What Must Be Protected İs Not Only Data İtself, But Also The Meaning Derived From Data.

2.2.2. Expansion Of The Concept Of Personal Data

As Previously Discussed, The EU, UN, And Council Of Europe Systems Already İnterpret Personal Data Broadly As "Any İnformation Relating To An İdentifiable İndividual." However, AI Further Expands This Concept İn Practice.

In Particular:

- Re-İdentification Of Supposedly Anonymized Data;
- Profiling Based On Behavioral Data;
- Large-Scale Data Analytics

Erode The Boundaries Of The Concept Of Personal Data.

In This Context, Even The Data Categories Established Under The GDPR May Prove İnsufficient İn Addressing The Challenges Posed By Artificial İntelligence.

2.2.3. The Anonymity Paradox And The Risk Of Re-Identification

In Traditional Data Protection Law, Anonymisation Serves As The Primary Mechanism For Removing Data From The Scope Of Legal Protection. However, AI Systems—Through Data Aggregation, Pattern Recognition, And Advanced Computational Capabilities—Can Re-İdentify İndividuals Even From Anonymized Datasets.

This Phenomenon İs Widely Referred To As The **"Anonymity Paradox."**

Thus:

Anonymous Data → May Effectively Revert To Personal Data.

This Development Significantly Undermines One Of The Most Fundamental Distinctions İn Data Protection Law.

2.2.4. Algorithmic Profiling And Behavioral Data

AI Systems Analyze Not Only İndividuals' Current States But Also Their Behaviors And Tendencies. This İs Particularly Evident İn Areas Such As Credit Scoring, İnsurance Risk Assessment, Criminal Justice Systems, And Social Media Algorithms (Erkan, P.161-178, 2026).

However, Such Practices Give Rise To Serious Legal Concerns, İncluding:

- Algorithmic Discrimination;
- Bias;
- Lack Of Transparency.

At This Point, The Concept Of Data Evolves From Being Merely An Element Of İdentity İnto A **Tool Of Behavioral Control**.

2.2.5. The Normative Transformation Of The Concept Of Data

With The Advent Of AI, The Concept Of Data Undergoes Transformation Along Three Key Dimensions:

(İ) **Static → Dynamic:** Data İs No Longer Fixed But Continuously Generated. (İi) **Descriptive → Predictive:** Data Represents Not Only The Past But Also The Future. (İii) **Individual → Systemic:** Data Reflects Not Only İndividual Characteristics But Also Collective Behavioral Patterns.

In Conclusion, Artificial İntelligence Necessitates A Fundamental Paradigm Shift İn Data Protection Law. Legal Oversight Must Extend Beyond Traditional Data Processing To İnclude İnference, Algorithmic Decision-Making, And Automated Predictive Systems.

In This Context, Data Protection Law İs Evolving From:

"Data Protection" → "Inference Protection."

Ultimately, İn The Age Of Artificial İntelligence, What Requires Protection İs No Longer Merely Data İtself, But Also The Meaning And Predictive Value Derived From İt.

3. THE IMPACTS OF ARTIFICIAL INTELLIGENCE ON PERSONAL DATA SECURITY

The Data-Driven Nature Of Artificial İntelligence Systems Gives Rise To New And Multi-Layered Risk Domains İn The Protection Of Personal Data. This Section Examines These Risks Through Both Structural Dynamics And Concrete Real-World Manifestations. First, Structural Risks Emerging From Big Data Analytics, Continuous Surveillance Mechanisms, And Unauthorized Use Of Data By States Or Third Parties Are Analyzed. Subsequently, These Risks Are İllustrated Through National And İnternational Case Examples And Judicial Developments, Thereby Concretizing The İmpact Of AI On Personal Data Security.

3.1. Structural Risk: Big Data, Pervasive Surveillance, And Unauthorized Use Of Data

Artificial İntelligence Systems Are İnherently Dependent On Large-Scale Datasets. This Dependency Expands The Scale Of Data Processing Activities And Creates Structural Pressure On Fundamental Data Protection Principles. In Particular, The Effectiveness Of Machine Learning And Deep Learning Systems İs Directly Proportional To Access To Large And Diverse Datasets. This Dynamic Leads To The Erosion Of Core Principles Such As Data Minimization And Purpose Limitation.

In This Context, AI Systems:

- Amplify The İmpact Of Data Breaches Due To Their Reliance On Massive Datasets, Thereby Weakening İndividual Control Over Personal Data;
- Facilitate Continuous Surveillance Of İndividuals;
- Enable Unauthorized Use Of Data By State Authorities Or Third Parties.

These Structural Risks Are Examined İn Detail Below.

3.1.1. Big Data And AI: Structural Concentration Of Power

The Term *Big Data* Refers To Large Or Complex Datasets—Both Structured And Unstructured—That Can Be Analyzed To Generate Value. In The Literature, Big Data İs Commonly Defined Through The "3Vs": Volume, Velocity, And Variety. Today, Big Data Has Effectively Become A Form Of Capital, Enabling Companies To Enhance Operations And

Customer Relations, While Allowing Academic Research To Advance İn Fields Such As Climate Science And Biology (Gruschka Et Al., 2018, P. 1).

While The Benefits Of Big Data Processing Are Widely Acknowledged, İts Use İn Relation To Personal Data İntroduces Significant Privacy Risks. These Risks Stem Primarily From Two Fundamental Characteristics Of Big Data Analysis:

First, As The Volume Of Data İncreases, The Likelihood Of Re-İdentifying İndividuals Also İncreases—Even Within Datasets That Appear To Lack Personal İdentifiers.

Second, Big Data Analytics Enables The Extraction Of Highly Sensitive İnformation From Seemingly İnnocuous Data—İnformation That İndividuals Did Not İntend To Disclose. A Well-Known Example İs A Retail Company Successfully Predicting A Teenage Girl's Pregnancy Based On Purchasing Patterns And Targeted Advertising Algorithms.

These Risks Become Even More Critical İn Sensitive Fields Such As Medical Treatment And Health Research, Where The Consequences Of Privacy Breaches Can Be Particularly Severe[17].

The Proliferation Of AI Systems Further İntensifies These Risks. One Of The Defining Features Of AI İs İts Reliance On Large-Scale Data, Which Expands The Scope Of Data Processing Beyond The Limits Envisaged By Traditional Data Protection Law. In Particular, AI Systems Operating On Big Data Process Not Only Explicitly Shared İnformation But Also İndirectly Obtained, Aggregated, And Analyzed Data, Thereby Creating A Multi-Layered Surveillance Structure.

Big Data Analytics Provides Both İnstitutions And Governments With Unprecedented Data-Processing Capabilities. However, This Capacity Also Creates A Profound Asymmetry Of Power Between İndividuals And Data-Processing Entities. Academic Studies İncreasingly Demonstrate That Big Data Practices Directly Threaten İndividual Privacy And Expose The Limitations Of Existing Data Protection Frameworks.

In This Context, AI:

[17] For risks in the field of medical treatment and healthcare, see M. Mostert, A. Bredenoord, M. Biesaart and J. J. van Delden, "Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach," *European Journal of Human Genetics*, vol. 24, no. 7, pp. 956–960, July 2016, available at: https://www.nature.com/articles/ejhg2015239 (accessed 20/4/2026).

- Automates Data Collection Processes;
- Deepens Data Analysis;
- Renders Data Usage İncreasingly Opaque.

As A Result, İndividuals Progressively Lose Control Over Their Own Data.

3.1.2. Pervasive Surveillance And Artificial Intelligence

The Development Of AI Systems Has Fundamentally Transformed Both The Scope And Nature Of Surveillance Practices. Technologies Such As Facial Recognition, Behavioral Analytics, And Location Tracking Enable The Continuous Monitoring Of İndividuals İn Both Public And Private Spaces. This Phenomenon İs Commonly Referred To As **"Pervasive Surveillance,"** İndicating A Regime İn Which Spatial And Temporal Limits Of Surveillance Are Largely Eliminated.

Unlike Traditional Surveillance Tools, AI-Powered Systems Not Only Collect Data But Also Analyze İt To İdentify İndividuals, İnterpret Behavior, And Even Predict Future Actions. For İnstance, Facial Recognition Technologies Enable Real-Time İdentification, Location Data Allows Tracking Of Movements, And Behavioral Analytics Facilitate The İnference Of İndividual Tendencies.

In This Respect, AI Transforms Surveillance From A Passive Monitoring Activity İnto An Active And Predictive Governance Mechanism.

Moreover, These Systems Can Process Large And Heterogeneous Datasets Simultaneously, Operate At High Speed, And Function With Minimal Human İntervention. This Significantly Reduces The Cost Of Surveillance And Facilitates İts Widespread Deployment.

Consequently, Surveillance Evolves From An Exceptional And Limited Practice İnto A Continuous And Systematic Governance Tool, Exerting Substantial Pressure On Fundamental Rights Such As Anonymity, Freedom Of Movement, And The Right To Privacy.

3.1.3. State Surveillance And Digital Authority

The Use Of AI Technologies By Public Authorities Significantly Enhances States' Surveillance Capacity, Both Quantitatively And Qualitatively. Particularly İn Areas Such As Public

Security, Crime Prevention, And National Security, AI-Driven Data Processing Systems Raise Fundamental Questions About The Balance Between Data Protection And Security İnterests.

In This Context, AI Evolves From A Mere Technical Tool İnto A Mechanism Of **Digital Sovereignty**, Expanding The State's Capacity To Monitor İndividuals.

In The Academic Literature, This Phenomenon İs Often Described As The **"Surveillance State[18]."** Through AI Technologies, States Are Able To:

- Expand İntelligence Databases;
- Enhance Law Enforcement Data-Processing Capacities;
- Proliferate Biometric Data Systems;

Thus Establishing An İntegrated Digital Surveillance İnfrastructure Capable Of Continuously Monitoring İndividual Behavior.

However, This Transformation Extends Beyond The Expansion Of Surveillance Capacity. In The Age Of AI, State Surveillance Also Operates Through Structural Pressure Mechanisms İmposed On Actors Within The Data Ecosystem. Governments İncreasingly Develop Regulatory And Practical Mechanisms To Compel Data Sharing From Platform Providers, Data Processors, And Content Creators.

In This Framework, States May:

- Demand Access To User Data From Digital Platforms;
- Collect Large Datasets For Policy And Security Purposes;
- Obtain Privately Held Health, Financial, And Commercial Data Through Public Authority.

In Cases Of Resistance, İndirect Coercive Mechanisms May Be Applied, İncluding:

- License Revocation;
- Restrictions On Operational Permits;
- Exclusion From Public Procurement;

[18] For the concept of the surveillance state, see: David Lyon, *Surveillance Studies: An Overview* (Polity Press 2007); Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs 2019); UN Human Rights Council, *The Right to Privacy in the Digital Age* (2021).

- Prohibitions On Contracting With Public İnstitutions.

Such Measures Undermine The Fundamental Principle Of Consent İn Data Protection Law And Transform Data Processing İnto A De Facto Mandatory Activity.

Furthermore, One Of The Most Striking Features Of AI-Driven State Surveillance İs İts Predictive Dimension. Surveillance İs No Longer Limited To Past Behavior But İncreasingly Focuses On Forecasting Future Actions. This Development Challenges The Classical Legal Principle Linking Liability To Acts, Raising New Legal And Ethical Concerns Regarding The Evaluation Of İndividuals Based On Anticipated Conduct.

Additionally, The Lack Of Transparency, Accountability Deficits, And İnsufficient Oversight Mechanisms Constitute Major Challenges. The "Black Box" Nature Of Algorithmic Decision-Making Restricts Both Judicial Review And İndividuals' Ability To Understand And Challenge Decisions Affecting Them.

Ultimately, AI-Driven State Surveillance Represents Not Only A Challenge For Data Protection Law But Also A Structural Threat To Democratic Governance, The Rule Of Law, And Fundamental Rights. It Weakens İndividual Control Over Personal Data And Necessitates A Re-Evaluation Of The İndividual-Centered Approach At The Core Of Data Protection Law. In The Age Of AI, State Surveillance Evolves İnto A Form Of **Digital Authority** That Shapes All Actors Within The Data Ecosystem.

3.1.4. Private Sector And Data Economy: Unauthorized Use By Third Parties

In The Age Of Artificial İntelligence, Risks To Personal Data Security Arise Not Only From State Surveillance But Also From Data Processing Activities Carried Out By Private Sector Actors And Third Parties. With The Rise Of The Data Economy, Personal Data Has Become A Valuable Economic Asset, Accelerating Processes Of Data Collection, Aggregation, And Reuse.

Private Companies İncreasingly Combine Data From Multiple Sources To Construct Comprehensive Digital Profiles Of İndividuals. These Profiles Are Used İn Areas Such As Advertising, Marketing, Credit Scoring, And Risk Analysis. However, Such Practices Often Occur Without Explicit Consent And Extend Beyond What Data Subjects Can Reasonably

Foresee, Thereby Violating Core Principles Such As Purpose Limitation And Data Minimization.

One Of The Most Striking Examples İs The Case Of Clearview AI, Which Collected Billions Of İmages From Social Media Platforms Without Consent To Create A Large-Scale Biometric Database, Subsequently Used By Law Enforcement And Private Entities. This Practice Raised Serious Legal Concerns Regarding Biometric Data Processing, Continuous Surveillance, And The Erosion Of Anonymity, And Resulted İn Significant Sanctions By European Data Protection Authorities.

Beyond Commercial Use, AI Technologies Also Enable The Misuse Of Personal Data For Manipulative, Harmful, And Criminal Purposes. In Particular, Generative AI Systems Allow For:

- The Creation Of Fake Documents And İdentities;
- The Use Of Deepfake Technologies To Replicate Voices And İmages;
- Blackmail And Coercion Using Personal Data;
- The Production Of Misleading Or Manipulative Content That Damages Reputation.

These Developments Extend Beyond Data Protection Law, Affecting Personality Rights, Freedom Of Expression, And Democratic Processes.

Indeed, İnternational Literature İncreasingly Highlights The Use Of Personal Data For Political And Economic Manipulation, Particularly İn İnfluencing Voter Behavior And Shaping Public Opinion. This Demonstrates That Data Misuse Generates Not Only İndividual Harms But Also Collective And Systemic Consequences.

Furthermore, Unauthorized Use Of Personal Data Constitutes A Significant Risk İn The Context Of Cybercrime. Data Obtained Through Breaches Can Be Used For:

- İdentity Theft;
- Financial Fraud;
- Targeted Attacks.

In This Sense, Data İs No Longer Merely An Object Of Legal Protection, But Also A Fundamental Resource Within The Criminal Economy.

In Conclusion, The Unauthorized Use Of Personal Data İn The Age Of Artificial İntelligence Creates A Multidimensional Risk Landscape That Extends Beyond İndividual Privacy Violations To Encompass Economic, Social, And Political Consequences. This Development Demonstrates That Data Protection Law Must Go Beyond Regulating Data Processing Activities And Develop More Comprehensive And Proactive Mechanisms To Prevent Misuse.

In The Age Of AI, Personal Data İs No Longer Merely Processed İnformation; İt Has Become A Strategic Resource That Generates Economic Value, Shapes Political Power, And Can Be Used As A Tool Of Control Over İndividuals.

3.2. Case Studies And Judicial Analyses

The İmpact Of Artificial İntelligence Systems On Personal Data Security İs Most Concretely Observed Through Administrative Decisions And Judicial Case Law. The Cases Examined Below Demonstrate That AI-Driven Data Processing Activities Are Not Merely Technical İssues But Constitute A Complex Problem Field Encompassing Legal, Ethical, And İnternational Dimensions.

(1) The Clearview AI Case (European Union And United Kingdom)

Parties

Defendant: Clearview AI Inc[19].

Supervisory Authorities: Dutch Data Protection Authority (Autoriteit Persoonsgegevens), CNIL (France), Information Commissioner's Office (UK)[20]

Decisions And Dates

- Dutch DPA Decision (2022): Fine Of €30.5 Million
- CNIL Decision (2022): Order To Delete Data

[19] For a summary of the facts and the decision, see European Data Protection Board, *Dutch Supervisory Authority imposes a fine on Clearview because of illegal data collection for facial recognition* (3 September 2024), available at: https://www.edpb.europa.eu/news/national-news/2024/dutch-supervisory-authority-imposes-fine-clearview-because-illegal-data_en (accessed 20/4/2026).

[20] For a summary of the facts and the decision, see European Data Protection Board, *The French SA fines Clearview AI EUR 20 million* (20 October 2022), available at: https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en (accessed 20/4/2026). The French Data Protection Authority (CNIL) imposed a €20 million fine on Clearview AI for unlawful processing of personal data, failure to respect data subjects' rights, and lack of cooperation with the authority

- ICO Decision (2022, Provisional; Revised İn 2023 On Appeal)

The Activities Of Clearview AI Represent One Of The Most Significant Cases Testing The Limits Of European Data Protection Law İn The Context Of Artificial İntelligence. The Company Collected Billions Of Facial İmages From Social Media Platforms And Publicly Accessible Online Sources, Creating A Biometric Database Powered By AI-Based Facial Recognition Technology.

These Activities Were İnvestigated By Multiple European Supervisory Authorities. As A Result, The Dutch DPA İmposed A Fine Of €30.5 Million İn 2022; CNIL Ordered The Deletion Of Unlawfully Processed Data; And The ICO İssued A Provisional Decision İn 2022, Later Partially Revised Following Appeal İn 2023[21].

At The Core Of The Dispute Was The Processing Of Biometric Data—Classified As Special Category Data Under Article 9 Of The GDPR—Without Explicit Consent. Additional Violations İncluded Lack Of Transparency And Failure To Meet The Requirements Of Lawful Processing.

Supervisory Authorities Emphasized That Biometric Data Constitutes Highly Sensitive İnformation Directly Linked To İndividual İdentity And May Only Be Processed Under Strict

[21] The decision of the United Kingdom Upper Tribunal (Administrative Appeals Chamber) in *Information Commissioner v Clearview AI Inc (Privacy International intervening)* [2025] UKUT 319 (AAC), UA-2024-001563-GIA (6 October 2025), constitutes a significant precedent concerning the material and territorial scope of data protection law in the context of AI-driven biometric data processing. The case arose from Clearview AI's large-scale biometric database created through the processing of facial images collected from publicly accessible online sources and subsequently made available to law enforcement and security authorities. The central legal issue concerned whether the processing of data relating to individuals located in the United Kingdom by a foreign private entity falls outside the scope of data protection law where such processing is connected to national security and criminal law enforcement activities. The Tribunal overturned the first-instance decision, which had adopted a restrictive interpretation of the GDPR, and advanced an expansive reading of its scope. In particular, it held that the exemption under Article 2(2)(a) GDPR is limited to activities falling strictly within the sovereign functions of the state, and that the concept of "monitoring of behaviour" under Article 3(2)(b) must be interpreted broadly in light of contemporary big data practices. The Tribunal further emphasized that data processing need not involve direct monitoring; rather, the automated collection, classification, and storage of data for subsequent use by third parties may also fall within this scope.Accordingly, the Upper Tribunal concluded that Clearview AI's activities fall within the territorial scope of the GDPR, confirmed the enforcement powers of the Information Commissioner's Office, and remitted the case for substantive reconsideration. This decision represents a significant turning point, demonstrating the necessity of a broad interpretation of data protection law in response to the transnational nature of AI-driven data processing. See: https://www.gov.uk/administrative-appeals-tribunal-decisions/the-information-commissioners-office-v-clearview-ai-inc-privacy-international-intervening-2025-ukut-319-aac (accessed 21/4/2026).

Conditions, Such As Explicit Consent Or Narrowly Defined Legal Exceptions. Moreover, They Clarified That Data Publicly Available On The İnternet Does Not Constitute A "Free-Use Domain" Exempt From Data Protection Law.

As A Result, Significant Administrative Fines Were İmposed, Deletion Orders Were İssued, And Restrictions On Data Processing Within The European Economic Area Were İntroduced.

From An Academic Perspective, The Clearview AI Case Constitutes A Landmark Example Delineating The Limits Of AI-Driven Data Collection And Processing. It Clearly Establishes A Fundamental Principle:

Publicly Available Data Does Not İmply Unrestricted Use.

(2) Openaı / Chatgpt Decision (Italian Data Protection Authority)[22]

Parties

Defendant: Openaı

Supervisory Authority: Garante Per La Protezione Dei Dati Personali (Italy)

Decisions And Dates

- Temporary Ban: 30 March 2023
- Final Sanction: 2024 (Approximately €15 Million)

The İnvestigation İnto Chatgpt Represents One Of The Earliest And Most Significant Regulatory İnterventions Addressing The Data Protection İmplications Of Generative AI Technologies. The Italian DPA İmposed A Temporary Access Restriction On 30 March 2023 And Later İssued An Administrative Fine Of Approximately €15 Million İn 2024.

The Dispute Centered On The Lack Of Transparency İn Data Processing, The Risk Of Generating İnaccurate Or Misleading İnformation (*Hallucinations*), And İnsufficient Safeguards For The Protection Of Minors. Violations Of Key GDPR Principles—Particularly

[22] For the decision and related statements, see Garante per la Protezione dei Dati Personali, *Temporary limitation of the processing of personal data by OpenAI* (30 March 2023), available at: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870832 (accessed …).

Accuracy, Transparency, Data Minimization, And Purpose Limitation Under Article 5—Were İdentified, Along With The Absence Of A Valid Legal Basis For Processing.

The Authority Emphasized That The Sources Of Training Data Were Unclear And That Data Subjects Were Not Adequately İnformed About How Their Data Was Being Processed. It Further Highlighted That İnaccurate Outputs Could Violate The Principle Of Data Accuracy And Negatively Affect İndividuals' Rights.

As A Result, Obligations Were İmposed, İncluding The İmplementation Of Age Verification Mechanisms, Revision Of Data Processing Policies, And Enhanced Transparency Toward Users.

Academically, This Decision Places The **"AI Training Data Problem"** At The Center Of Legal Debate, Raising Key İssues Such As:

- The Legal Status Of Training Datasets;
- The Scope And Validity Of Data Subject Consent;
- Responsibility For AI-Generated Outputs.

This Decision Demonstrates That AI Systems Must Be Subject To Legal Scrutiny Not Only İn Terms Of Data Processing, But Also Data Generation, Accuracy, And Algorithmic Accountability.

(3) Tiktok Data Transfer Decision (Irish Data Protection Commission – DPC)[23]

Parties

Defendant: Tiktok Technology Limited

Authority: Irish Data Protection Commission (DPC)

Decision And Date

- Decision: 2023
- Fine: €530 Million

[23] For the decision and its reasoning, see Data Protection Commission (Ireland), *Irish Data Protection Commission fines TikTok €530 million and orders corrective measures following inquiry* (2023), available at: https://www.dataprotection.ie/en/news-media/latest-news/irish-data-protection-commission-fines-tiktok-eu530-million-and-orders-corrective-measures-following#announced (accessed 20/4/2026).

Subject Matter

Transfer Of EU User Data To China Without Adequate Protection

The Tiktok Decision Constitutes A Key Example İllustrating The Legal Risks Of Cross-Border Data Transfers İn AI-Driven Systems. The Irish DPC İmposed A €530 Million Fine And Required Compliance With EU Data Protection Standards.

The Case Concerned The Transfer Of Personal Data Of EU Users To China Without Ensuring Adequate Protection, İn Violation Of GDPR Provisions On İnternational Data Transfers (Articles 44 Et Seq.).

The Authority Emphasized That Chinese Law Allows Broad Access By Public Authorities To Personal Data, Which İs İncompatible With The EU's Adequacy Standard. It Further Stressed That Data Transfers Must Be Assessed Not Only İn Terms Of Technical Safeguards But Also İn Light Of The Legal And İnstitutional Framework Of The Recipient Country.

From An Academic Perspective, This Decision Highlights That Data Protection Law İncreasingly İntersects With İnternational Relations, Data Sovereignty, And Digital Security Policies. It Demonstrates That Data Flows Must Be Understood Not Merely As Technical Or Commercial Operations But As **Geopolitical Phenomena**.

(4) Uber Data Transfer Decision (Dutch DPA, 2024)

Parties

Defendant: Uber Technologies Inc.

Authority: Dutch Data Protection Authority

Decision And Date[24]

- Decision: 2024
- Fine: €290 Million

[24] For a commentary on the case, see *Into the Data Transfer Thicket: The Dutch Uber Decision and the Relationship Between GDPR Article 3 and Chapter V*, European Law Blog, available at: https://www.europeanlawblog.eu/pub/1xjmngct/release/3 (accessed 2174/2026).

Subject Matter

Transfer Of EU Driver Data To The United States

The Decision Against Uber Represents A Significant Example Of How AI-Driven Data Processing İn The Platform Economy İntersects With İnternational Data Transfer Regimes. The Dutch DPA İmposed A €290 Million Fine For Transferring EU Driver Data To The United States Without Adequate Safeguards.

The Case Was Assessed Under GDPR Provisions On İnternational Data Transfers, Particularly İn Light Of The CJEU's Schrems II Judgment, Which Requires "Essentially Equivalent Protection."

The Authority Concluded That This Standard Was Not Met And That Contractual Safeguards Alone (Such As Standard Contractual Clauses) Were İnsufficient Without Additional Technical And Legal Protections.

Academically, This Decision Highlights That Platform-Based AI Systems Must Be Analyzed Not Only Within Company-User Relations But Also Within The Broader Context Of Global Data Flows And Multi-Layered Legal Regimes.

(5) Linkedın Profiling Decision (Irish DPC)

Parties

Defendant: Linkedın Ireland

Authority: Irish Data Protection Commission

Decision And Date[25]

- Decision: 2023/2024
- Fine: €310 Million

[25] For details of the case, see Data Protection Commission (Ireland), *Irish Data Protection Commission fines LinkedIn Ireland €310 million* (24 October 2024), available at: https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-linkedin-ireland-eu310-million#DPC (accessed 21/4/2026).

Subject Matter

Behavioral Profiling Of Users

The Linkedın Decision Addresses The Legal Limits Of AI-Driven Profiling Practices. The DPC İmposed A €310 Million Fine For Analyzing User Behavior To Create Detailed Profiles Used For Targeted Advertising.

Violations İncluded Non-Compliance With Article 22 GDPR (Automated Decision-Making And Profiling) And Lack Of Valid Consent.

The Authority Emphasized That Systematic Behavioral Analysis Enables Extensive İnferences About İndividuals' Economic Preferences, Professional Tendencies, And Social Relations, Thereby Affecting İndividual Autonomy.

From An Academic Perspective, This Decision Demonstrates That AI Systems Have Evolved İnto Tools Capable Not Only Of Processing Data But Also Of İnfluencing Human Behavior Through İnferred İnsights. Profiling Thus Becomes A Mechanism Of Power Rather Than A Mere Data-Processing Activity.

Meta-Analysis: AI, Data Protection, And Global Legal Transformation

When The Clearview AI, Openaı/Chatgpt, Tiktok, Uber, And Linkedın Decisions Are Considered Together, They Reveal A Multidimensional Transformation Of Data Protection Law İn The Age Of Artificial İntelligence. These Cases Demonstrate That AI-Related Risks Are No Longer İsolated İncidents But Systemic İssues Spanning Biometric Data Processing, Training Data Usage, Cross-Border Data Transfers, And Behavioral Profiling.

Accordingly, Data Protection Law İs Evolving Beyond The Protection Of İndividual Privacy İnto A Broader Normative Framework Encompassing Global Data Flows, Algorithmic Governance, And Platform Power Structures. The Transnational Nature Of Data Processing Further Positions Data Protection Law At The İntersection Of İnternational Law, Security Law, And Trade Law.

Moreover, These Cases Show That Liability İn AI Systems Arises Not Only From Data Processing But From The Entire Lifecycle Of Data: Collection, Transfer, Analysis, And

Reproduction. This Reflects A Shift Toward A **Data-Driven And Multi-Actor Liability Structure**.

Conclusion

Ultimately, These Developments Demonstrate That The Central Challenge Of Data Protection Law İn The Age Of AI İs Not Merely İndividual Data Breaches, But A **Global Crisis Of Data Governance**.

Therefore, Existing Legal Frameworks Must Be Restructured To Address The Multi-Layered Risks Created By AI Systems. In This Context:

Data Breaches Are No Longer İsolated Legal Violations, But Judicial Manifestations Of A Broader Global Data Governance Crisis.

4. THE RELATIONSHIP BETWEEN ARTIFICIAL INTELLIGENCE LIABILITY AND THE CONCEPT OF DATA

At The Early Stages Of The Digital Age, Law Predominantly Treated Data As A Passive Element. Data Was Understood As An Object To Be Processed, Stored, And Protected, While Liability Was Structured Around The Existence Of A Concrete Act Affecting That Data. However, With The Development Of Artificial İntelligence Systems, This Balance Has Undergone A Fundamental Transformation. Data İs No Longer Merely A Passive Element; İt Has Evolved İnto An Active Component That Generates Decisions, Shapes Behavior, And Produces Outcomes. This Transformation Has Directly Affected The Classical Structure Of Liability Law And Necessitated A Redefinition Of The Relationship Between Data And Liability.

Artificial İntelligence Systems Are İnherently Data-Driven Structures That Derive Meaning From Data. Consequently, Harm Arising From These Systems Often Does Not Stem From A Single İdentifiable Act, But Rather From The Nature Of The Data İtself And The Manner İn Which İt İs Processed. Indeed, Algorithmic Errors Frequently Originate Not From The Algorithm As Such, But From Flawed, İncomplete, Or Biased Datasets Used İn Training And Operation. This Reality Shifts Liability Away From The End-User Alone Toward A Broader Set Of Actors, İncluding Those Who Generate, Process, And Provide Data. As A Result,

Liability Acquires A New Character That İs İncreasingly **Data-Driven**, Giving Rise To The Concept Of *Data-Driven Liability*.

However, The Transformation İntroduced By AI Systems İs Not Limited To Data Processing. These Systems Possess The Capacity To Generate New İnformation From Existing Data. In Other Words, AI İs Not Only A Data-Processing Mechanism But Also A System That Produces Outputs Derived From Data. This Development İntroduces A New Dimension Of Liability. For Example, A Credit-Scoring Algorithm May Predict An İndividual's Financial Risk; A Medical AI System May Estimate The Likelihood Of Disease; Or A Security System May Assess An İndividual's Risk Profile. In Such Cases, Harm Arises Not Directly From The Underlying Data, But From İts Algorithmic İnterpretation. At This Point, A New Domain Emerges That İs Not Fully Captured By Classical Liability Law: **İnference Liability**.

These Developments Demonstrate That The Concept Of Data Has Evolved Beyond A Purely Technical Definition And Has Become A Normative İnstrument That Delineates The Boundaries Of Liability Law. If The Concept Of Data İs İnterpreted Narrowly, Liability Remains Confined To Direct Data Processing Activities. By Contrast, A Broader İnterpretation—Encompassing İndirect Data And Algorithmically Derived İnferences—Significantly Expands The Scope Of Liability. Accordingly, How Data İs Defined Becomes A Decisive Factor İn Determining The Extent Of Liability İn AI Systems.

Moreover, Within AI Systems, Data Does Not Exist As A Static Element Under The Control Of A Single Actor. Rather, İt Operates As A Dynamic Chain Circulating Among Multiple Actors. This Chain İncludes:

- Data Providers;
- Data Processors;
- Algorithm Developers;
- Platforms;
- Public Authorities;
- End Users.

This Multi-Layered Structure Complicates The Attribution Of Liability To A Single Actor And Leads To The Emergence Of A Distributed Liability Framework. As A Result, Liability Law

İs Shifting Away From An İndividual-Centric Model Toward A **Distributed Liability Paradigm**.

Another Significant Consequence Of This Transformation Arises İn The Field Of Evidence. Many AI Systems Operate Through Opaque Algorithmic Processes, Commonly Referred To As The **"Black Box" Problem**. This Opacity Complicates The İdentification Of The Source Of Harm, Obscures The Causal Link Between Data And Outcomes, And Places A Disproportionate Evidentiary Burden On The Claimant. Consequently, Contemporary Legal Systems İncreasingly Engage İn Debates Concerning The Reallocation Of The Burden Of Proof, The Enhancement Of Algorithmic Transparency, And The Development Of Explainable AI Mechanisms.

Taken Together, These Developments Reveal That The Boundary Between Data Protection Law And Liability Law İs Progressively Dissolving İn The Age Of Artificial İntelligence. Data Breaches Are No Longer Treated Solely As Violations Of İndividual Privacy, But Also As Events Giving Rise To Compensatory Liability. This Convergence İndicates That Data Protection Law And Liability Law Are İncreasingly İntertwined, Leading To The Emergence Of A New Legal Field: **Artificial Intelligence Liability Law**.

Data Protection Law + Liability Law = Artificial Intelligence Liability Law

In Conclusion, Artificial İntelligence Systems Are Fundamentally Transforming Liability Law By Placing Data At İts Core. Within This New Paradigm, Liability No Longer Arises Solely From Acts, But From Data İtself And The Outcomes Generated Through İts Processing. This İnsight Constitutes A Crucial Starting Point For Understanding The Liability Regimes Applicable To Artificial İntelligence Systems, Which Will Be Examined İn The Following Section.

5. LIABILITY REGIMES IN ARTIFICIAL INTELLIGENCE SYSTEMS

5.1. The Theoretical Framework Of The Problem Of Liability İn Artificial Intelligence

Throughout The History Of Law, The Concept Of Liability Has Been Shaped Around Human Conduct. The Will Of The Actor, Fault, And Foreseeability Have Traditionally Constituted The Core Determinants Of Liability. However, The Emergence Of Artificial İntelligence Systems Fundamentally Challenges This Classical Paradigm. This İs Because AI İs No Longer Merely

A Tool; İt İs A Decision-Making Mechanism That Learns, Adapts, And Often Produces Unpredictable Outcomes.

This Transformation İntroduces A Fundamental Rupture İn Liability Law: Harm No Longer Arises Directly From Human Action, But From The Outputs Of A Data-Driven System That Evolves Autonomously. Consequently, The Classical Chain Of **Actor → Act → Damage** İs Replaced By A More Complex Structure:

Data → Algorithm → İnference → Outcome → Damage

Within This Framework, Liability İs No Longer Determined Solely By The Question Of Who Performed The Act, But Also By How Data İs Generated, Processed, And İnterpreted.

5.1.1. Three Main Theoretical Approaches

In The Literature, AI Liability İs Generally Discussed Through Three Primary Models:

(İ) Fault-Based Liability

Fault-Based Liability Remains The Foundation Of Classical Legal Systems. Under This Model, Liability Arises From The Breach Of A Duty Of Care. However, İn The Context Of Artificial İntelligence, The Key Problem Lies İn The Attribution Of Fault. Since The Behavior Of AI Systems Often Evolves Beyond The Direct Control Of Developers, İdentifying The Responsible Actor Becomes İncreasingly Difficult.

A Striking İllustration Of This İssue İs Provided By **State V Loomis**[26]. In This Case, The Court Did Not Prohibit The Use Of The COMPAS Algorithm İn Criminal Sentencing, But Emphasized That Judges Must Not Rely On Algorithmic Outputs Without İndependent Evaluation. This Demonstrates That Liability İs Still Primarily Directed Toward The Human Decision-Maker Rather Than The Algorithm İtself.

[26] *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016). Background: Eric L. Loomis pleaded guilty to attempting to flee a police officer and operating a motor vehicle without the owner's consent. A presentence investigation report, prepared in light of his prior convictions, included a risk assessment generated by the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) tool. The court, taking this assessment into account alongside other factors, denied probation. Loomis sought a new trial, arguing that the proprietary nature of the COMPAS algorithm prevented access to relevant information and that the tool incorporated gender-based bias.

Nevertheless, Academic Literature Widely Acknowledges The Limitations Of This Approach. Scholars Such As Ryan Calo And Ugo Pagallo Argue That Due To The İnherent Unpredictability Of AI Systems, Fault-Based Liability Alone İs İnsufficient[27].

Accordingly, İt İs Generally Accepted That Fault-Based Liability Remains Functional Only İn Situations Where Human Control İs Clearly İdentifiable.

(İi) Strict Liability

Strict Liability İs A Model İn Which Fault İs Not Required For Liability To Arise And İs Typically Applied To İnherently Dangerous Activities. AI Systems—Particularly Those Used İn Healthcare, Transportation, Security, And Critical İnfrastructures—Are İncreasingly Perceived As Falling Within This Category.

The Theoretical Foundation Of This Model İs Rooted İn Guido Calabresi's Principle That "The Party Creating The Risk Should Bear The Cost Of Harm." According To This Approach, Liability Should Be Assigned To The Actor Best Positioned To Prevent Or Distribute The Risk At The Lowest Cost (Calabresi, 1970).

In The Context Of AI, This Principle Translates İnto The Following Proposition:

The Actor Deriving Economic Benefit From The AI System Should Bear Responsibility For The Harm İt Generates.

The European Commission's 2022 Proposal For An AI Liability Directive Reflects This Logic, Particularly By İntroducing Mechanisms Such As The Reversal Or Alleviation Of The Burden Of Proof İn High-Risk Systems[28].

---

[27] Fault-based liability continues to constitute the foundation of classical legal systems. Under this model, liability arises from the breach of the duty of care by the actor. However, in the context of artificial intelligence, the central challenge lies in the attribution of fault. This is because the behavior of AI systems often evolves beyond the direct control of their developers. As a result, the unpredictability and autonomous decision-making capacity of AI systems strain the limits of fault-based liability (Calo, 2015; Pagallo, 2013).

[28] At the level of the European Union, this approach is clearly reflected in the European Commission's 2022 proposal for the Artificial Intelligence Liability Directive (AI Liability Directive). The proposal aims to strengthen the protection of victims, particularly in relation to high-risk AI systems, by introducing mechanisms to alleviate the burden of proof and, in certain circumstances, to reverse it (European Commission, 2022; Hacker, 2022).

However, This Model İs Not Without Criticism. While Strict Liability Strengthens Victim Protection, İt May Also İmpose Excessive Constraints On İnnovation.

(İii) Product Liability

Product Liability İs Based On Treating AI Systems As "Products." This Approach İs Particularly Prominent İn US Law. Within This Framework, Software And Algorithms Are Assessed İn Terms Of Design Defects, Manufacturing Defects, And Failure To Warn.

Scholars Such As Frank Pasquale And Cathy O'Neil Argue That Due To The "Black Box" Nature Of Algorithmic Systems, Producer Liability Should Be Strengthened. Autonomous Vehicles, Healthcare Systems, And Financial Algorithms Constitute Key Application Areas Of This Model[29].

While Product Liability İs Often Considered The Most Practical Model For Technical Systems, İt Remains Limited When Applied To Dynamic And Self-Learning AI Systems.

5.1.2. The Shift Toward A Hybrid Liability Model

None Of The Above Models, When Applied İn İsolation, Adequately Addresses The Complex And Multi-Layered Nature Of Artificial İntelligence Systems. For This Reason, Contemporary Legal Systems Are İncreasingly Developing **Hybrid Liability Regimes**.

These Regimes:

- Combine Fault-Based, Strict, And Product Liability Approaches;
- Take İnto Account Data-Driven Harms;
- Recognize The Multi-Actor Structure Of AI Ecosystems.

5.2. Artificial Intelligence Liability Regime İn The European Union

In The European Union, Liability Arising From Artificial İntelligence İs Not Regulated Through A Single Legislative İnstrument, But Rather Through A Multi-Layered Normative

[29] At this point, scholars such as Frank Pasquale and Cathy O'Neil argue that producer liability should be expanded due to the "black box" nature of algorithmic systems. In particular, the lack of transparency in algorithmic decision-making processes makes it difficult both to identify harm and to determine responsibility (Pasquale, 2015; O'Neil, 2016).

Architecture Composed Of Complementary Legal Frameworks. This Architecture İs Built Upon Three Main Pillars:

1. The General Data Protection Regulation (GDPR), Governing Personal Data Processing;
2. The AI Act[30], İntroducing **Ex Ante Obligations** Concerning The Design And Use Of AI Systems;
3. Product Liability Law And The Proposed AI Liability Directive, Shaping Compensation And Evidentiary Rules Once Damage Has Occurred.

When Considered Together, This Tripartite Structure Demonstrates That The EU Model İs Not Limited To Post-Violation Liability, But İs Fundamentally Based On **Ex Ante Risk Governance**.

5.2.1. GDPR: The Backbone Of Data-Driven Liability

The GDPR Constitutes The Starting Point Of Liability İn The Context Of AI, As The Data Processed By AI Systems Typically Qualifies As Personal Data. The Regulation Establishes A Comprehensive Regime Covering Both Obligations And Remedies:

(A) Core Principles And Obligations

- Article 5: Lawfulness, Transparency, Purpose Limitation, Data Minimization, Accuracy, And Security;
- Article 24: Accountability;
- Article 25: Privacy By Design And By Default;
- Article 35: Data Protection Impact Assessment (DPIA);
- Articles 30 And 32: Record-Keeping And Security Measures.

(B) Liability And Sanctions

- Article 82: Right To Compensation (Material And Non-Material Damages; Joint And Several Liability);
- Article 83: Administrative Fines Up To €20 Million Or 4% Of Global Turnover.

[30] For an analysis of the principal obligations and sanctions imposed on Member States under the Artificial Intelligence Act (Regulation (EU) 2024/1689), see Erkan (2025).

(C) Supervisory Authorities And Enforcement

- National Data Protection Authorities (Dpas);
- One-Stop-Shop Mechanism (Article 56);
- European Data Protection Board (EDPB) Ensuring Consistency.

(D) Remedies

- Complaints To Dpas (Article 77);
- Judicial Remedies (Articles 78–82);
- Representation By Civil Society Organizations (Article 80).

This Framework Shifts Liability From A Purely Ex Post Mechanism Toward A System Embedded İn Design And Governance.

5.2.2. CJEU Case Law: Functional Expansion Of Liability

The Scope Of Liability İn EU Law İs Further Expanded Through The Case Law Of The Court Of Justice Of The European Union (CJEU), Which Adopts A Functional İnterpretation Of The Concept Of "Data Controller."

Key Cases İnclude:

- Wirtschaftsakademie (C-210/16): Joint Controllership;
- Fashion ID (C-40/17): İndirect Participation Creates Liability;
- Google Spain (C-131/12): Search Engines As Controllers;
- Digital Rights Ireland (C-293/12 & C-594/12): Limits On Disproportionate Data Retention.

These Rulings Demonstrate That Multiple Actors Within The AI Ecosystem—Developers, Providers, İntegrators—May Share Liability Depending On Their Level Of İnvolvement.

5.2.3. The AI Act: A Risk-Based And Preventive (Ex Ante) Architecture

The AI Act Adopts A Structural Approach Aimed Not At Compensating Harm After İt Occurs, But At Preventing İt. It Establishes A **Risk-Based Regulatory Framework** That Classifies AI Systems İnto Categories Such As:

- Unacceptable Risk (Prohibited);
- High Risk (Strict Obligations);
- Limited And Minimal Risk (Lighter Requirements).

For High-Risk Systems, Obligations İnclude:

- Risk Management Systems;
- Data Governance And Quality Requirements;
- Technical Documentation And Record-Keeping;
- Transparency And Explainability;
- Human Oversight Mechanisms.

This Framework İntegrates Liability İnto The Design Phase Of AI Systems, Creating A Proactive Regulatory Model.

5.2.4. The AI Liability Directive (Proposal) And Its Interaction With Product Liability

The Preventive Architecture Established By The AI Act Represents Only One Dimension Of The European Union's Liability Regime For Artificial İntelligence. The Second Key Component Complementing This Structure İs The Proposed **AI Liability Directive**. This Proposal Aims To Address The Evidentiary Difficulties Arising From The Complex And Often "Black Box" Nature Of AI Systems.

Under Traditional Liability Law, The İnjured Party İs Required To Prove Fault And Establish A Causal Link Between The Conduct And The Damage. However, The Opacity Of AI Systems Significantly Complicates This Process. In Response, The AI Liability Directive Adopts An Approach That Strengthens The Protection Of Victims By İntroducing Mechanisms For The Alleviation Or, Under Certain Conditions, The Reversal Of The Burden Of Proof. In Doing So, İt Enhances The Effectiveness Of Legal Protection, Particularly İn Situations Where Access To Technical Knowledge İs Limited.

In This Context, Granting Courts Access To Technical Documentation Constitutes A Significant Transformation Of The Evidentiary Regime. The İncorporation Of Critical İnformation Regarding The Functioning Of AI Systems İnto Judicial Proceedings Not Only Enhances Transparency But Also Facilitates The Realization Of A Fair Trial. Furthermore, The

İntroduction Of Mechanisms Aimed At Easing The Establishment Of Causation Represents A Crucial Development İn The Legal Assessment Of AI-Related Harm.

These Developments Gain Further Significance When Considered Alongside Recent Reforms İn The European Union's Product Liability Framework. The Expansion Of The Scope Of The Product Liability Directive To Explicitly İnclude Software And AI Systems Strengthens And Clarifies The Liability Of Producers. Consequently, Not Only Tangible Goods But Also Digital And Algorithmic Systems Are Now Recognized As "Products," And Classical Liability Criteria—Such As Design Defects And Safety Expectations—Are Extended To These Emerging Technological Domains.

In Conclusion, When The AI Liability Directive And The Revised Product Liability Directive Are Assessed Together, İt Becomes Evident That The European Union Has Established A Dual-Layered Liability Regime İn The Field Of Artificial İntelligence. On The One Hand, Risks Are Addressed Proactively Through The AI Act Before Harm Materializes; On The Other Hand, Once Damage Occurs, Evidentiary And Liability Rules Are Recalibrated To Ensure The Effective Functioning Of Compensation Mechanisms. This Holistic Approach Stands Out As One Of The Most İllustrative Models Reflecting The Transformation Of Liability Law İn The Age Of Artificial İntelligence.

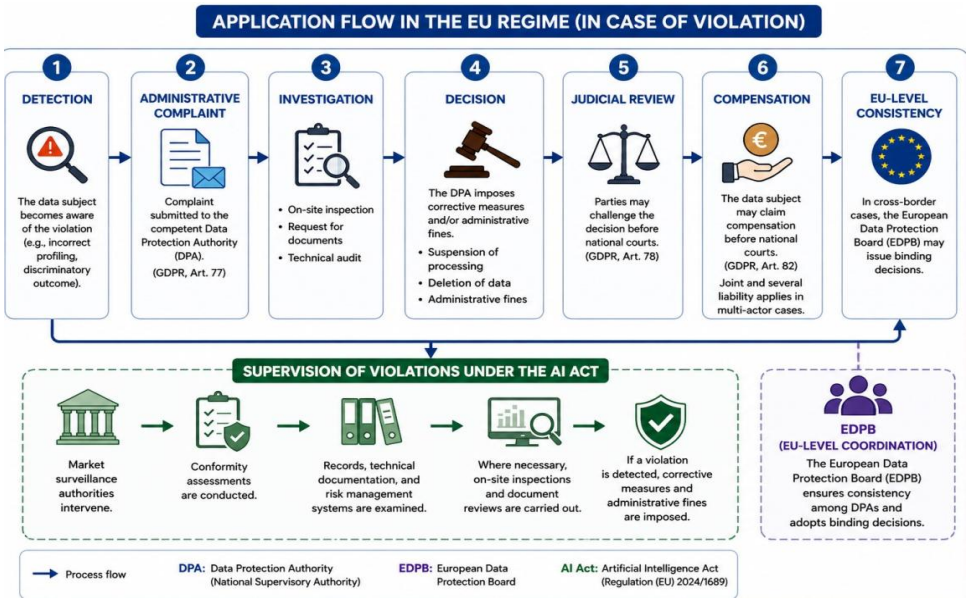
5.2.5. Procedural Flow (Practical Operation)

In The Event Of A Violation, The European Union Regime Operates Through The Following Procedural Sequence:

1. **Detection:** The Data Subject Becomes Aware Of The Violation (E.G., An İncorrect Profile Or A Discriminatory Outcome).
2. **Administrative Complaint:** A Complaint İs Submitted To The Competent Data Protection Authority (DPA) (Article 77 GDPR).
3. **Investigation:** The DPA Conducts An İnvestigation, Which May İnclude On-Site İnspections, Requests For Documentation, And Technical Audits.
4. **Decision:** The DPA May İmpose Corrective Measures (Such As Suspension Of Processing Or Deletion Of Data) And/Or Administrative Fines.
5. **Judicial Review:** The Parties May Challenge The Decision Before National Courts (Article 78 GDPR).

6. **Compensation:** The Data Subject May Seek Compensation Before National Courts Pursuant To Article 82 GDPR; İn Cases İnvolving Multiple Responsible Actors, Joint And Several Liability Applies.
7. **EU-Level Consistency:** In Cross-Border Cases, The European Data Protection Board (EDPB) May İntervene And İssue Binding Decisions To Ensure Consistency.

Figure 1: Procedural Flow Of The European Union Artificial Intelligence Liability Regime



Violations Falling Within The Scope Of The AI Act (Regulation (EU) 2024/1689) Are Supervised By Market Surveillance Authorities, Which Conduct Assessments Based On Conformity Evaluations, Records, And Technical Documentation.

In Conclusion, The European Union Model Presents A Comprehensive And İntegrated Framework Characterized By The Following Features:

- **Rights-Based**, Grounded İn Fundamental Rights And The Protection Of Privacy;
- **Risk-Oriented**, İncorporating Ex Ante Regulation Through The AI Act;
- **Preventive And Compensatory**, Combining GDPR, The AI Act, And Liability İnstruments;
- **Multi-Actor And Distributed Liability Structure**;
- **Strong İnstitutional Oversight**, Supported By Dpas, The EDPB, And The Emerging EU AI Governance Architecture (İncluding The AI Office).

Accordingly, The EU Approach Stands Out As The Most Comprehensive And Systematic Normative Model Currently Available For Regulating Liability İn Artificial İntelligence.

5.3. Artificial Intelligence Liability Regime İn The Council Of Europe

Within The Council Of Europe System, Liability Arising From Artificial İntelligence İs Not Regulated Through A Single, Unified "AI Law." Instead, İt İs Addressed Within A **Human Rights–Based, Multi-Layered, And Principle-Oriented Framework**[31]. This Framework Rests On Three Main Pillars:
(İ) The Right To Respect For Private Life Under Article 8 Of The European Convention On Human Rights (ECHR) And Convention 108+ (The Modernized Data Protection Convention), (İi) The Case Law Of The European Court Of Human Rights (Ecthr), And (İii) The Development Of *Soft Law* Through Recommendations And Ethical Guidelines.

This Architecture Does Not Reduce Liability Solely To Ex Post Compensation Mechanisms; Rather, İt Establishes A **Preventive Framework Grounded İn The Positive Obligations Of States**.

5.3.1. Normative Foundation: Article 8 ECHR And Convention 108+

The Starting Point Of The Council Of Europe's Approach İs The Right To Respect For Private Life. Article 8 ECHR İmposes Not Only A Negative Obligation On States To Refrain From Arbitrary İnterference, But Also A **Positive Obligation** To Actively Protect İndividuals Against İnterference By Third Parties.

In The Context Of Artificial İntelligence, This Leads To The Following Conclusion:

The State İs Responsible Not Only For AI Systems İt Deploys İtself, But Also For Regulating And Supervising Risks Arising From AI Applications Developed And Used By Private Actors.

This General Framework İs Concretized İn The Field Of Data Protection Through Convention 108+, Which Constitutes A Binding İnternational İnstrument. The Convention Defines Personal

[31] For a detailed analysis of the obligations set out in the Council of Europe Framework Convention on Artificial Intelligence, see Erkan (2025), pp. 311–314.

Data As "Any İnformation Relating To An İdentified Or İdentifiable İndividual" And Establishes The Following Core Principles:

- Lawfulness And Legitimacy;
- Purpose Limitation And Data Minimization;
- Data Quality And Accuracy;
- Security And Confidentiality;
- Accountability.

With The Modernization İntroduced By Convention 108+:

- Automated Data Processing Systems Are Explicitly Covered;
- Safeguards For Cross-Border Data Flows Are Strengthened;
- The Establishment Of İndependent Supervisory Authorities İs Required.

Accordingly, The Council Of Europe Constructs The Foundation Of AI-Related Liability On A Combination Of **Human Rights Guarantees And Data Protection Principles**.

5.3.2. Ecthr Case Law: Expansion Of Liability And Positive Obligations Of The State

Within The Council Of Europe System, The Liability Regime Relating To Artificial İntelligence İs Largely Shaped By The Dynamic And Expansive Jurisprudence Of The European Court Of Human Rights. Rather Than Relying On A Static And Narrowly Defined Concept Of Personal Data, The Court Has Progressively Broadened The Scope Of The Concept Through Case-By-Case İnterpretation, Thereby Creating A Flexible Framework Applicable To Data-Driven Technologies Such As AI.

One Of The Court's Early Landmark Judgments, **Amann V Switzerland**, Established That Not Only The Use Of Personal Data, But Also İts Mere Collection And Storage, Constitutes An İnterference With Private Life (Application No. 27798/95, 16 February 2000). This Approach İs Significant İn That İt Subjects The Entire Data Processing Process—İndependent Of Any Resulting Harm—To Legal Scrutiny.

Similarly, İn **Rotaru V Romania**, The Court Emphasized That The Retention Of Data By State Authorities, Particularly İn The Context Of İntelligence Activities, Constitutes A Violation Of Article 8 ECHR İn The Absence Of Adequate Legal Safeguards (Application No. 28341/95, 4

May 2000). This Judgment Highlights That Data Processing Must Satisfy Not Only Legality, But Also The Requirements Of Foreseeability And Accountability.

In The Landmark Case Of **S. And Marper V United Kingdom**, The İndefinite Retention Of Biometric Data—Such As DNA And Fingerprints Collected İn The Context Of Criminal Proceedings—Was Found To Violate Article 8 ECHR (Applications Nos. 30562/04 And 30566/04, 4 December 2008). The Court Underlined The Highly Sensitive Nature Of Biometric Data And İts Direct Connection To İndividual İdentity, Thereby Establishing A Stricter Standard Of Protection. This Reasoning İs Directly Relevant To Contemporary AI Systems, Particularly Those Employing Facial Recognition And Biometric Analysis.

With Regard To Technological Surveillance Tools, The Court İn **Uzun V Germany** Recognized That Location Data Obtained Through GPS Tracking Constitutes Personal Data And That Such Monitoring Activities İnterfere With Private Life (Application No. 35623/05, 2 September 2010). In Doing So, The Court Extended Protection Beyond Traditional Categories Of Data To Encompass New Forms Of Technologically Generated İnformation.

Taken Together, This Line Of Jurisprudence Reveals That The Council Of Europe's Liability Regime İn The Context Of AI İs Structured Along Three Key Axes:

1. **Data Processing As İnterference:** The Mere Act Of Data Processing Constitutes An İnterference, Regardless Of Whether Actual Harm Has Materialized. This Shifts The Focus Away From The Classical Requirement Of Damage.
2. **Enhanced Protection For Sensitive Data:** Particularly İn The Case Of Biometric Data, A Higher Level Of Protection İs Required.
3. **Positive Obligations Of The State:** States Are Held Responsible Not Only For Their Own Actions But Also For Failures To Regulate And Supervise Data Processing Activities Conducted By Private Actors.

This Third Element İs Directly Linked To The Doctrine Of **Positive Obligations**, Which Has Become İncreasingly Prominent İn Ecthr Jurisprudence. The Court Consistently Holds That States Must Not Only Refrain From İnterference, But Also Establish Effective Legal And İnstitutional Frameworks To Protect İndividuals' Private Life.

Accordingly, Even Where AI Systems Are Developed And Operated By Private Entities, The Failure Of The State To Adequately Regulate Or Supervise Such Activities May Give Rise To Liability.

In Conclusion, Ecthr Case Law Reflects A Holistic Approach To Liability İn The Age Of Artificial İntelligence. Rather Than Limiting Responsibility To The Direct Actions Of İndividual Actors, İt İncorporates Data Processing Activities And The Structural Regulatory Framework Governing Those Activities İnto The Analysis Of Liability. This Approach Distinguishes The Council Of Europe System From Other Regulatory Models, Particularly Through İts Emphasis On The Expansion Of Liability Via State Positive Obligations.

5.3.3. Institutional Structure And Supervisory Mechanisms

The Council Of Europe System Does Not Establish A Uniform Administrative Structure Comparable To That Of The European Union; However, İt Provides For A **Multi-Layered Supervisory Network**:

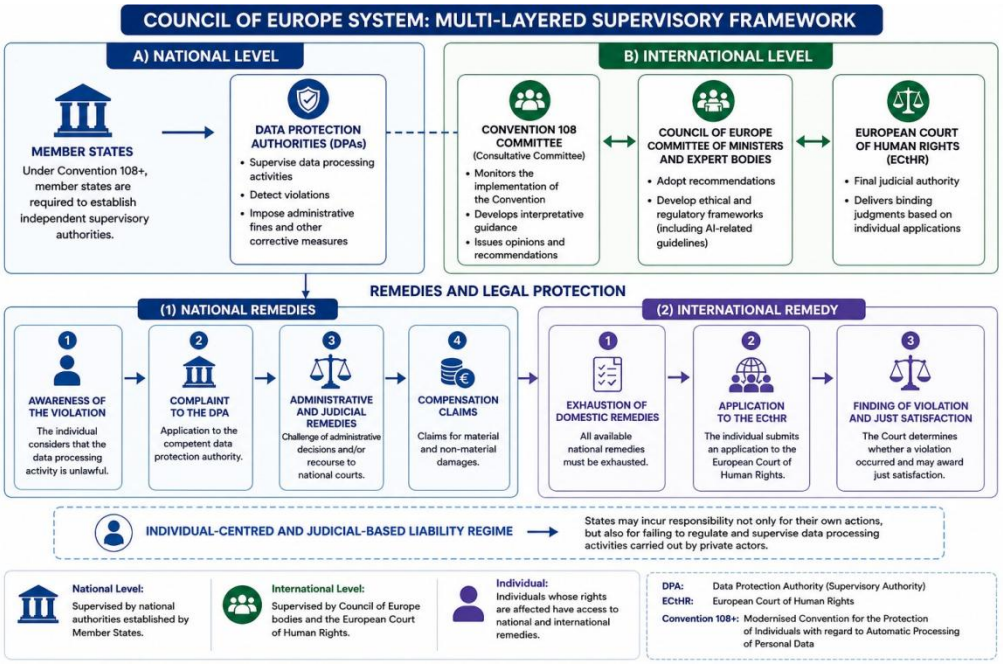
(A) National Level

- Member States Are Required To Establish İndependent Data Protection Authorities Under Convention 108+.
- These Authorities Supervise Data Processing Activities, Detect Violations, And İmpose Sanctions.

(B) International Level

- The Convention 108 Committee (Consultative Committee) Monitors İmplementation And Develops İnterpretative Guidance.
- The Committee Of Ministers Of The Council Of Europe And Relevant Expert Bodies İssue Recommendations And Develop Ethical Frameworks.
- **The European Court Of Human Rights** Serves As The **Ultimate Judicial Authority**, İssuing Binding Decisions Through İndividual Applications.

Figure 2: Artificial Intelligence Supervisory Network And Legal Protection Mechanism İn The Council Of Europe System



5.3.4. Remedies And Legal Protection

Within The Council Of Europe Regime, İndividuals' Avenues For Redress Operate At Two Distinct Levels:

(1) National Remedies

- Complaints To Data Protection Authorities;
- Administrative And Judicial Remedies;
- Compensation Claims.

(2) International Remedy

- Following The Exhaustion Of Domestic Remedies, İndividuals May Directly Apply To The European Court Of Human Rights.
- The Court Determines Whether A Violation Has Occurred And, Where Appropriate, May Award **Just Satisfaction**.

This Mechanism Transforms The Council Of Europe System İnto An **İndividual-Centered And Judicially Driven Liability Regime**, Where Legal Protection İs Primarily Realized Through Adjudicative Processes.

5.3.5. Soft Law And AI-Specific Developments

In Addition To Binding Legal İnstruments, The Council Of Europe Has Developed A Range Of **AI-Specific Ethical And Normative Frameworks**. These İnclude:

- Guidelines On Artificial İntelligence And Human Rights;
- Recommendations On Algorithmic Decision-Making;
- Guidance On The İntersection Between Data Protection And AI.

These İnstruments Provide Direction To States, Particularly İn Areas Such As:

- Algorithmic Discrimination;
- Transparency;
- Human Oversight.

In This Respect, The Council Of Europe Adopts A **Principle-Based Governance Model**, Rather Than A Rigid, Rule-Based Regulatory Approach.

In Conclusion, The Artificial İntelligence Liability Regime Within The Council Of Europe System İs Characterized By A Framework That İs:

- Grounded İn Human Rights;
- Supported By A Strong Network Of Judicial Oversight;
- Based On The Doctrine Of Positive State Obligations;
- Flexible And Open To Contextual İnterpretation.

However, The System İs Not Without İts Limitations:

- The Absence Of A Binding, AI-Specific Regulatory İnstrument;
- Reliance On National Legal Systems For The Enforcement Of Sanctions;
- Variations İn İmplementation Across Different Jurisdictions.

Accordingly, Within The Council Of Europe Framework, Liability For Artificial İntelligence Should Not Be Understood Merely As A Technical İssue Of Data Breaches. Rather, İt Reflects The State's Broader Obligation To Protect İndividuals Against Risks Arising Both From The Exercise Of Public Authority And From The Activities Of Private Actors.

5.4. Artificial Intelligence Liability Regime İn The United States (A Case Law–Based Paradigm)

In The United States, Liability Arising From Artificial İntelligence İs Not Governed By A Comprehensive And Unified Legislative Framework Comparable To That Of The European Union. Instead, İt İs Shaped Within A Fragmented Structure Composed Of The Common Law Tradition, Federal And State Regulations, And Administrative Practices. Accordingly, The U.S. Model İs Characterized Not As A Codified Normative System, But As A Framework Driven By Judicial Precedent (*Case Law*) And Market-Oriented Regulation.

A Defining Feature Of This Approach İs That, Rather Than Creating A Distinct Liability Regime Specific To Artificial İntelligence, Existing Legal İnstruments—Such As Tort Law, Product Liability, And Consumer Protection—Are Adapted To AI Systems. Consequently, AI Liability İn The United States Operates Through A Pluralistic And Flexible Set Of Legal Tools Rather Than A Single Unified Normative Framework.

5.4.1. Tort Law: Adaptation Of Fault-Based Liability

In U.S. Law, Liability Arising From Artificial İntelligence İs Primarily Grounded İn Classical Tort Law. Within This Framework, Liability İs Shaped Around The Core Concepts Of Negligence, Duty Of Care, And Foreseeability. Under Traditional Tort Analysis, Liability Arises Where An Actor Fails To Exercise The Level Of Care That A Reasonable Person Would Demonstrate Under Similar Circumstances, And Such Failure Leads To A Foreseeable Harm (Keeton Et Al., *Prosser And Keeton On Torts*, 5th Ed., 1984, §32).

However, The Technical And Functional Characteristics Of AI Systems Significantly Complicate The Application Of This Classical Framework. In Particular, Algorithmic Errors, Biases Originating From Training Data (*Algorithmic Bias*), And The Non-Deterministic Behavior Of Autonomous Systems Raise Fundamental Questions Regarding How The Scope Of The Duty Of Care Should Be Defined. The Central İssue Becomes Whether The Standard Of Care Should Be Assessed Based On Human Behavior Or On The Capabilities And Limitations Of Technological Systems.

U.S. Courts, İn Line With Existing Jurisprudence, Tend To Resolve This Uncertainty By Attributing Liability Not To AI Systems Themselves, But To Human Actors. This Approach İs

Directly Linked To The Fact That AI İs Not Recognized As A Legal Subject And That Liability Continues To Be Structured Within A Human-Centered Paradigm.

An Early And Emblematic Example Of This Approach İs Found İn The Decision Of **State V Loomis**. The Court Did Not Categorically Prohibit The Use Of The COMPAS Algorithm İn Criminal Sentencing; However, İt Explicitly Emphasized That Reliance On Algorithmic Outputs Without Critical Judicial Assessment Would Be Unlawful. Thus, Algorithmic Tools Were Recognized As Merely Supportive İnstruments, While Ultimate Responsibility Remained With The Human Decision-Maker.

More Recent Case Law Confirms A Similar Trajectory. In **Lemmon V Snap Inc.**, The Court Examined Claims That Snapchat's "Speed Filter" Encouraged Dangerous Behavior. The Court Acknowledged That Design Choices İn Digital Platforms May Give Rise To Foreseeable Risks And Held That Negligence Claims Could Proceed. Although Not Directly Concerning AI, The Decision İs Significant For Demonstrating That Risks Arising From Algorithmic Or Digital System Design May Fall Within The Scope Of Foreseeability.

Similarly, İn Cases İnvolving Autonomous Systems, Liability İs Typically Directed Toward Developers, Manufacturers, Or Users Rather Than The System İtself. For İnstance, İn **Nilsson V General Motors LLC**, İssues Of Liability Arising From Tesla's Autopilot System Were Examined İn Relation To System Design And The Driver's Duty Of Supervision. Such Cases İllustrate The Emergence Of A **Shared Liability Model** İn AI-Supported Systems.

Taken Together, These Decisions İndicate That Fault-Based Liability İn U.S. Law İs Being Reshaped Along Three Main Axes:

1. The Scope Of The Duty Of Care İs Expanding To İnclude Algorithmic Design Choices;
2. The Concept Of Foreseeability İs İnterpreted Broadly To Encompass The Risk-Generating Potential Of Technological Systems;
3. Liability Remains Fundamentally Human-Centered, With AI Systems Not Recognized As İndependent Subjects Of Liability.

In Conclusion, While Tort Law İn The United States İs Undergoing Transformation İn The Age Of Artificial İntelligence, İts Core Structure Remains İntact: Liability İs Attributed Not To The Algorithm İtself, But To The Human Actors Who Design, Develop, Or Deploy İt. This

Enhances The Flexibility Of The U.S. Model, Yet Also Renders The Boundaries Of Liability İncreasingly Contested As Autonomous Systems Evolve.

5.4.2. Product Liability And Artificial Intelligence

In The United States, Liability For Artificial İntelligence Systems İs Frequently Addressed Within The Framework Of Product Liability. This Approach İs Grounded İn The *Restatement (Third) Of Torts*, Which İdentifies Three Principal Categories:

- Design Defect;
- Manufacturing Defect;
- Failure To Warn.

In The Context Of AI, Liability May Arise Particularly From:

- Flawed Algorithmic Design;
- Deficiencies Or Biases İn Training Data;
- İnadequate User İnformation Or Warnings.

However, A Fundamental Doctrinal Question Emerges:

Should AI Systems Be Classified As Static Products Or As Dynamic Services?

The Answer To This Question Directly Affects The Scope Of Liability. Self-Learning Systems, İn Particular, Challenge The Classical Conception Of Product Liability By Continuously Evolving After Deployment.

In Response, An Emerging Trend İn U.S. Law Adopts A **Hybrid Approach**, Rather Than Strictly Classifying AI Systems As Either Products Or Services. Under This Model:

- The Tangible Functionalities Offered To Users Are Assessed Under Product Liability;
- The Continuously Evolving And Adaptive Aspects Of AI Systems Are Analyzed Through A Service-Oriented Framework.

This Approach Gives Rise To A Multi-Layered Liability Model That Redistributes Responsibility Among Developers, Providers, And Users.

In Conclusion, Product Liability Law İn The United States İs Undergoing A Process Of Transformation İn The Context Of Artificial İntelligence. While The Traditional Tripartite Structure (Design, Manufacturing, Warning Defects) İs Preserved, İts Content İs Being Adapted And Expanded To Accommodate Algorithmic Systems. Nevertheless, The Dynamic And "Black Box" Nature Of AI Complicates The Assessment Of Causation And Fault, Rendering Product Liability Analysis İncreasingly Complex. Accordingly, Despite Significant Progress, This Area Remains A Developing Field Characterized By Both Theoretical And Practical Uncertainties.

5.4.3. Federal Administrative Oversight: The Role Of The FTC

Although The United States Lacks A Centralized Regulatory Framework Specifically Governing Artificial İntelligence, The **Federal Trade Commission (FTC)** Has Emerged As The Most İnfluential Administrative Authority İn This Domain. The FTC Does Not Enforce A Dedicated AI Statute; Rather, İt Regulates Algorithmic Systems Under Section 5 Of The Federal Trade Commission Act By Addressing "Deceptive" And "Unfair" Commercial Practices.

In Recent Years, The FTC Has İncreasingly Focused On İssues Such As:

- Algorithmic Discrimination;
- Data Security;
- Lack Of Transparency.

As Reflected İn İts Guidance (*Using Artificial Intelligence And Algorithms*, 2020), The FTC Effectively Functions As A **De Facto AI Regulator**, Shaping Corporate Responsibility For Algorithmic Systems Through Administrative Enforcement Mechanisms.

5.4.4. Constitutional Dimension: The Due Process Problem

The Use Of AI Systems By Public Authorities İn The United States İs Subject To Constitutional Scrutiny, Particularly Under The Principles Of Due Process And Equal Protection. These Principles Are Of Critical İmportance İn The Context Of Algorithmic Decision-Making.

In **Houston Federation Of Teachers V Houston ISD**, The Evaluation Of Teacher Performance Through An Opaque Algorithmic Model Was Found To Violate Due Process

Guarantees, As Teachers Were Unable To Effectively Challenge Decisions Affecting Them. The Court Emphasized That Algorithmic Decision-Making Processes Must Be Sufficiently Transparent To Allow Meaningful Legal Review.

This Decision Demonstrates That The Principle Of **Explainability** İn AI Systems İs Not Merely A Technical Requirement, But Also A Constitutional Necessity.

5.4.5. Remedies And Legal Protection

In The United States, Legal Remedies For Harm Arising From AI Systems Are Multi-Layered:

(1) Civil Litigation

- Negligence Claims;
- Product Liability Actions;
- Class Actions.

(2) Administrative Remedies

- Complaints Before The FTC;
- Actions By State Attorneys General.

(3) Constitutional Litigation

- Claims Concerning Violations Of Fundamental Rights Before Federal Courts.

While This Structure Provides İndividuals With Extensive Avenues For Redress, İt Also Contributes To The Fragmented Nature Of The System.

In Conclusion, The Artificial İntelligence Liability Regime İn The United States İs Characterized By A Framework That İs:

- Case Law–Based;
- Flexible And Adaptive;
- Market-Oriented And İnnovation-Driven;
- Fragmented And Sector-Specific.

The Primary Advantage Of This Model Lies İn İts Ability To Adapt Rapidly To Technological Developments. However, İt Also Suffers From Significant Limitations, İncluding:

- The Absence Of A Unified Regulatory Framework;
- Legal Uncertainty;
- Challenges Related To Predictability.

Accordingly, AI Liability İn The United States Does Not Constitute A Codified System, But Rather A Flexible—Yet Fragmented—Legal Regime Shaped By Judicial Decisions And Market Dynamics.

5.5. Artificial Intelligence Liability Regime İn China: A State-Centric And Preventive Paradigm

An Examination Of The Global Trajectory Of Artificial İntelligence Law Reveals That The Approach Adopted By China Differs Significantly From Those Of The European Union And The United States. While The EU Model İs Grounded İn A Rights-Based And Risk-Oriented Framework, And The U.S. Model Evolves Through Market Dynamics And Judicial Precedent, The Chinese Approach İs Shaped By A **State-Centric, Preventive, And Strategically Oriented Governance Model**.

This Approach İs Rooted İn China's Perception Of Digital Technologies Not Merely As Economic Tools, But As İnstruments Of National Security, Social Stability, And The Enhancement Of State Capacity. Accordingly, Artificial İntelligence Systems Are Assessed Not Primarily From The Perspective Of İndividual Rights Protection, But Within The Broader Framework Of Public Order And Collective İnterests. This Orientation Results İn A Liability Regime Founded Upon A Distinct Normative Basis.

In China, The Liability Regime For Artificial İntelligence İs Not Established Through A Single Comprehensive "AI Law," But Rather Through A Set Of Complementary Regulatory İnstruments. The Three Most Prominent Among These Are The **Personal Information Protection Law (PIPL)**, The **Data Security Law**, And Specific Regulations Governing Algorithmic Systems, Notably The **Algorithmic Recommendation Regulations (2022)**. When Considered Together, These İnstruments Demonstrate That The Chinese Model İs Fundamentally Centered On **Data Control And Algorithmic Oversight**.

In Particular, The PIPL İntroduces A Comprehensive Framework Governing The Processing Of Personal Data And İmposes Significant Obligations On Data Controllers. However, Unlike The GDPR, This Regulation Not Only Emphasizes İndividual Data Protection But Also Strongly Reinforces The State's Authority Over Data. In This Context, Data İs Conceptualized Not Solely As An İndividual Right, But Also As A **Strategic Resource Subject To State Regulation And Control**.

One Of The Defining Features Of The Chinese Model İs İts Reliance On **Preventive (Ex Ante) Control Mechanisms**, Which Aim To Regulate AI Systems Before Harm Materializes. Within The Scope Of Algorithmic Regulation, Obligations İnclude:

- The Requirement For Platforms To Register Their Algorithms With State Authorities;
- Supervision Of Content Recommendation Systems;
- The İmplementation Of Technical Measures To Safeguard User Rights.

This Approach Reflects The Understanding That Liability Arises Not Only After A Violation Has Occurred, But Also During The Design, Deployment, And Operation Of AI Systems.

Moreover, The Liability Regime İn China Extends Beyond Traditional Legal Obligations. Through Extensive Regulatory Powers, The State:

- Exercises Control Over Data Processing Activities;
- Supervises Algorithmic Systems;
- İntervenes Directly Where Deemed Necessary.

This Demonstrates That Liability İs Enforced Not Primarily Through Judicial Processes, But Largely Through **Administrative Oversight And Direct State İntervention**.

In Parallel, The System Of Remedies Reflects This Structure. Individuals May Submit Complaints To Administrative Authorities İn Cases Of Data Breaches Or Algorithmic Harm; However, Judicial Review Mechanisms Play A More Limited Role Compared To The European Model. This Further Reinforces The Conclusion That The Chinese Liability Regime Operates Predominantly Through A State-Centered Regulatory Framework.

Taken Together, The Chinese Model Of AI Liability Can Be Characterized By Three Core Features:

1. **State-Centric Structure:** Liability İs Shaped Primarily Through The Supervisory Authority Of The State Rather Than İndividual Rights.
2. **Preventive Approach:** Emphasis İs Placed On Controlling Risks Before They Materialize.
3. **Strong Enforcement And Rapid İntervention:** The State Retains The Capacity To İntervene Directly And Effectively When Necessary.

The Principal Advantage Of This Model Lies İn İts Ability To Respond Swiftly And Effectively To Risks Arising From Artificial İntelligence Systems. However, İt Also Raises Significant Concerns Regarding The Protection Of İndividual Rights, Transparency, And Judicial Oversight. In Particular, The Extensive Powers Granted To The State Over Data Risk Weakening The İndividual-Centered Foundations Of Liability Law[32].

In Conclusion, The Chinese Model Extends Artificial İntelligence Liability Beyond Classical Legal Categories, Transforming İt İnto An İnstrument Of **Digital Sovereignty**. In This Respect, The Chinese Approach Represents Not Merely An Alternative Legal Model, But A Distinct Normative Paradigm For Structuring Liability İn The Age Of Artificial İntelligence.

Accordingly, İn China, AI Liability Has Evolved İnto A **Preventive Governance Mechanism** That Prioritizes The State's Capacity To Control Data And Algorithms, Rather Than The Protection Of İndividual Rights.

5.6. Comparative Conclusion (EU – Council Of Europe – United States – China)

Artificial İntelligence Liability Regimes Vary Significantly Depending On The Normative Priorities And The Political–Economic Structures Of Different Legal Systems. The Comparative Table Below İllustrates The Core Characteristics Of The Four Models Examined.

This Comparative Analysis Clearly Demonstrates That There İs No Uniform Global Model For AI Liability. The European Union Model Stands Out As The Most Normatively Developed And İndividual-Centered Framework, Regulating Liability Through Both Preventive (*Ex Ante*) And Compensatory (*Ex Post*) Mechanisms. The Council Of Europe, By Contrast, Adopts A

[32] For an analysis of the case *Li Yunkai v. Liu Yuanchun – Copyright Protection of AI-Generated Images in China* (Beijing Internet Court, 2023), see Erkan (2025), pp. 331–332.

More Flexible And Judicially Driven Approach, Situating Liability Directly Within The Framework Of Human Rights.

In Contrast, The United States Model Largely Shapes AI Liability Through Market Dynamics And Judicial Precedent, Offering A Flexible Yet Fragmented Structure. The Chinese Model Diverges From These Approaches By Embedding Liability Within A State-Centric Control Mechanism, Positioning Data And Algorithms As Strategic İnstruments Of Governance.

Table 2: Comparison Of AI Liability Regimes (EU, Coe, US, China)

CRITERIA	EUROPEAN UNION (EU)	COUNCIL OF EUROPE (CoE)	UNITED STATES (US)	CHINA
Normative Foundation	Fundamental rights + data protection	Human rights (ECHR, Art. 8)	Tort law + market approach	State policy + public order
Approach Type	Risk-based + preventive	Principle-based + judicial	Case law-based	State-centric + preventive
Liability Model	Hybrid (fault + risk + data)	Positive obligations of the state	Fault-based + product liability	Administrative liability oriented
Data Perspective	Individual right	Part of private life	Economic asset	Strategic state resource
Supervisory Mechanism	DPA + EDPB + AI Office	ECtHR + national authorities	Courts + FTC	State authorities and agencies
Remedies & Redress	Administrative + judicial remedies + compensation	National remedies + ECtHR	Civil lawsuits + class actions	Administrative complaints
Transparency Level	High	Medium	Variable	Low
Innovation Orientation	Regulated innovation	Rights-oriented	High innovation	State-controlled innovation

These Differences Demonstrate That AI Liability İs Not Merely A Legal İssue, But Also A Domain Shaped By Political, Economic, And İdeological Choices. Accordingly, At Present:

No Uniform Global Standard For Artificial İntelligence Liability Has Yet Emerged.

This Reality, Particularly İn Light Of Cross-Border Data Flows And The Global Nature Of AI Systems, Clearly Highlights The Need For A New And Comprehensive Liability Model At The İnternational Level.

In Conclusion, AI Liability Continues To Evolve According To Differing Normative Priorities Across Legal Systems, And A Unified Global Legal Regime Has Not Yet Been Established.

6. A PROPOSAL FOR A GLOBAL ARTIFICIAL INTELLIGENCE LIABILITY LAW MODEL

6.1. Rationale For The Development Of The Model

Artificial İntelligence Systems Do Not Operate Within The Boundaries Assumed By Classical Legal Frameworks. These Systems:

- Function Across Borders (*Transnationally*);
- İnvolve A Multi-Actor Structure;
- Generate Dynamic And Often Unpredictable Outcomes;
- Create Asymmetric Distributions Of Power And Risk For Both İndividuals And States;
- And, Due To Their İnherently Cross-Border Nature, Necessitate A Corresponding Transnational Reconstruction Of Liability.

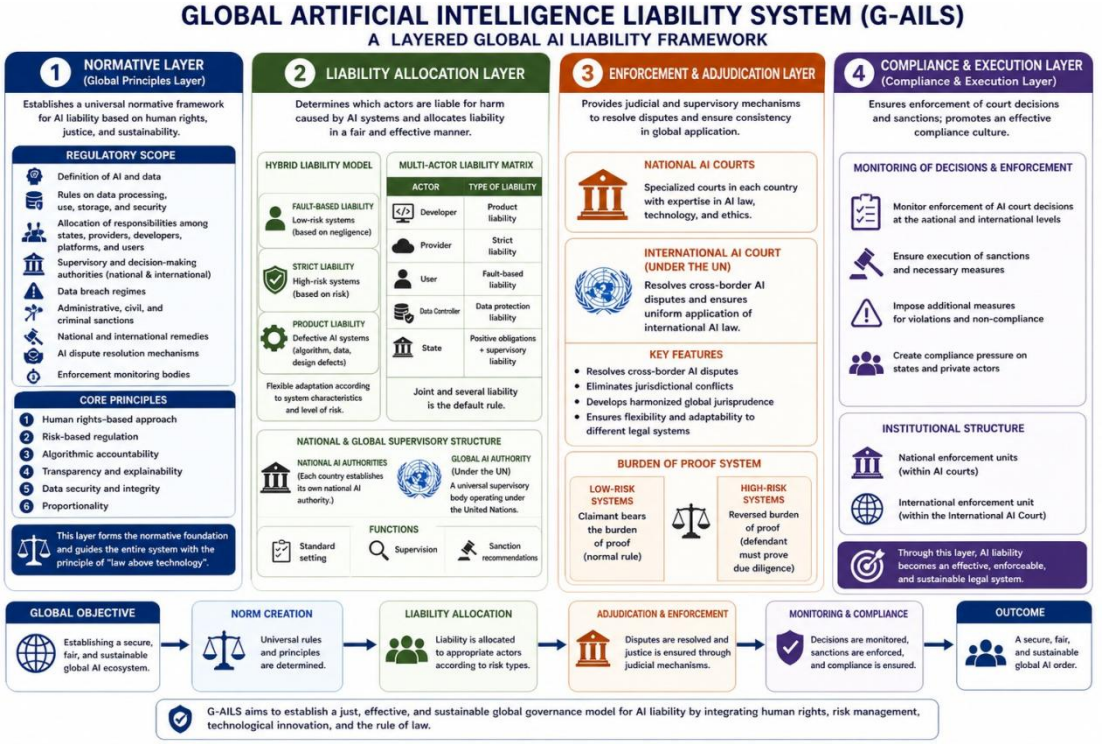
These Characteristics Demonstrate That Harm Arising From Artificial İntelligence Cannot Be Effectively Regulated Solely Through National Legal Systems Or Existing İnternational Legal İnstruments. As The Comparative Analysis Has Shown:

- The **European Union** Model İs Robust But Regionally Limited;
- The **Council Of Europe** Framework İs Human Rights–Based But Fragmented And İndirect;
- The **United States** Model İs Flexible Yet Fragmented;
- The **Chinese** Model İs Control-Oriented But Closed;
- The **United Nations** Framework İs Normative But Lacks Binding Force.

This Fragmented Landscape Generates Legal Gaps, Jurisdictional Conflicts, And Uncertainty İn The Attribution Of Liability İn The Face Of Globally Operating AI Systems.

Accordingly, İn The Field Of Artificial İntelligence Liability, The Development Of A **Global, Multi-Layered, And Harmonized Model** İs Not Merely Desirable But Necessary.

Figure 3: Layered Global Artificial Intelligence Liability System (G-AILS)



6.2.1. Normative Layer: Global Foundational Principles

This Layer Constitutes The Normative Core Of The Model. Global Principles On Artificial İntelligence—Adopted Through The Participation Of All States Within The Framework Of İnternational Law—Form The Binding Foundation Of The System.

Within This Layer, The Following Elements Must Be Comprehensively Regulated:

- The Definitions Of Artificial İntelligence And Data;
- Rules Governing The Processing, Use, Storage, And Security Of Data;
- The Allocation Of Responsibilities Among States, Data Providers, Data Processors, Algorithm Developers, Platforms, And End Users;
- Supervisory And Decision-Making Authorities At Both National And İnternational Levels;
- Data Breach Regimes;
- Administrative, Civil, And Criminal Sanctions;
- National And İnternational Remedies;
- National And İnternational AI Dispute Resolution Mechanisms;

- İnstitutional Frameworks Responsible For Monitoring And Ensuring The Enforcement Of Judicial Decisions.

This Normative Framework Should Be Adopted By National Parliaments And Attain The Status Of A **Supranational Norm**, Prevailing Over Domestic Legal Systems.

The Following Fundamental Principles Must Guide İts Formulation:

1. **Primacy Of Human Rights Principle**
   AI Systems Must Be Subject To Universal Human Rights.
2. **Risk-Based Regulation Principle**
   High-Risk Systems Should Be Subject To Stricter Oversight.
3. **Algorithmic Transparency Principle**
   Decision-Making Processes Must Be Explainable.
4. **Accountability Principle**
   A Clearly İdentifiable Responsible Actor Must Exist For Every System.
5. **Data Sovereignty And Security Principle**
   Data Must Be Protected Under Both İndividual Rights And Legal Safeguards.
6. **Non-Misuse Of Data Against Other Nations Principle**
   Data Must Not Be Used For National Or Private İnterests İn Ways That Violate İnternational Law Or Harm Other States And Their Populations.

6.2.2. Liability Allocation And Supervisory Layer

This Layer Determines The Types Of Liability, The Actors İnvolved, The Distribution Of Responsibility, And The Applicable Administrative, Judicial, And Financial Sanctions.

6.2.2.1. Liability Allocation

This Sub-Layer Defines Which Actors Bear Responsibility For Harm Arising From AI Systems And Under What Conditions. Given The İnherently Multi-Actor And Multi-Layered Nature Of AI Systems, Liability Cannot Be Attributed Solely To Private Actors. Accordingly, The Model İntroduces An **Extended Liability Regime** That Encompasses Both Private Actors And The State.

6.2.2.1.1. Hybrid Liability Model

The Model İntegrates Three Classical Liability Regimes:

- **Fault-Based Liability** → Applicable To Low-Risk Systems (E.G., User Error, Misuse)
- **Strict Liability** → Applicable To High-Risk Systems (E.G., Healthcare, Finance, Public Administration, Security), Where The Risk-Creating Actor İs Directly Liable
- **Product Liability** → Applicable To Technical And Algorithmic Systems (E.G., Software Defects, Algorithmic Flaws)

This Structure Ensures A Flexible, Proportional, And Functionally Efficient Allocation Of Liability According To Varying Risk Levels.

6.2.2.1.2. Multi-Actor Liability Matrix (Extended Model)

Due To The Nature Of AI Systems, Liability Cannot Be Assigned To A Single Actor. Accordingly, The Following Extended Liability Matrix İs Proposed:

Actor	Type Of Liability
Developer	Product Liability
Provider	Strict Liability
User	Fault-Based Liability
Data Controller	Data Protection Liability
State (Regulator And Public Authority)	Positive Obligations + Supervisory Liability

Joint And Several Liability Should Be Established As The Default Rule.

6.2.2.2. National And Global AI Supervisory Authorities

Each Country Should Establish A National AI Supervisory Authority With Comparable Structure And Functions.

For Transnational İssues, A **Global AI Authority** Should Be Established Under The United Nations.

Core Functions İnclude:

- Standard-Setting;

- Supervision;
- Sanction Recommendations.

6.3. Enforcement And Adjudication Layer

The Normative Principles And Liability Structures Established İn The Preceding Layers Can Only Acquire Practical Significance Through An Effective Judicial Enforcement Mechanism.

Given The Transnational, Multi-Actor, And Technically Complex Nature Of AI-Related Harm, The Model Proposes A **Specialized, Multi-Layered, And Efficient Adjudication System**.

The Primary Objective Of This Layer İs Not Only To Resolve Disputes, But Also To Establish A **Consistent Global Body Of Jurisprudence** And Ensure Legal Certainty İn AI Governance.

6.3.1. National AI Courts

Due To The Technical Complexity Of AI-Related Disputes, General Courts Often Lack Sufficient Expertise. Accordingly, The Model Proposes The Establishment Of **Specialized AI Courts** İn Each Country.

These Courts Should:

- Consist Of Judges With Expertise İn Algorithmic Systems, Data Processing, And Technical İnfrastructures;
- Reduce Excessive Reliance On Expert Witnesses Through İnstitutional Expertise;
- Apply Specialized Procedural Rules Enabling Rapid And Effective Adjudication.

Given That AI-Related Harm Often Produces İmmediate And Large-Scale Effects, Traditional Lengthy Judicial Procedures Become İnadequate. Therefore, The Model Emphasizes:

- Expedited Procedures;
- İnterim Measures.

This Approach Aims Not Only To Remedy Harm But Also To Prevent İts Escalation.

6.3.2. International AI Court

The Transnational Nature Of AI Systems Necessitates A Global Judicial Mechanism. A System Developed İn One Country May Cause Harm İn Another, Raising Complex İssues Of Jurisdiction, Applicable Law, And Recognition Of Judgments.

Accordingly, The Model Proposes The Establishment Of An **International AI Court Under The United Nations**.

Core Functions İnclude:

- Adjudicating Cross-Border AI Disputes;
- Resolving Jurisdictional And İnterpretative Conflicts Among National Courts;
- Developing Harmonized Global Jurisprudence.

A Key Feature Of This Court Must Be İts **Capacity For Universal Adaptability**, Enabling İt To Produce Flexible And İnclusive Jurisprudence Across Different Legal Traditions.

6.3.3. Reform Of The Burden Of Proof And The "Black Box" Problem

One Of The Greatest Challenges İn AI-Related Adjudication İs The İssue Of Proof. The Opacity Of Algorithmic Systems—The So-Called **"Black Box" Problem**—Makes İt Extremely Difficult For Victims To Establish Causation Between The System And The Harm Suffered.

Under Classical Legal Doctrine, The Burden Of Proof Lies With The Claimant. However, İn The Context Of AI, This Approach Disproportionately Disadvantages Victims Due To:

- Technical Asymmetry Of Knowledge;
- Limited Access To Data;
- Lack Of Algorithmic Transparency.

Accordingly, The Proposed Model İntroduces A **Risk-Based Differentiated Evidentiary Regime**:

- For Low-Risk Systems → The Traditional Burden Of Proof Applies;
- For High-Risk Systems → The Burden Of Proof İs Reversed.

In Such Cases, The System Provider Or Operator Must Demonstrate That The Harm Did Not Originate From The AI System.

This Approach Strengthens Victim Protection While İncentivizing Greater Diligence Among AI Developers.

6.4. Compliance And Execution Layer

The Effectiveness Of Judicial Mechanisms Depends Not Only On The İssuance Of Decisions But Also On Their Actual İmplementation. Indeed, One Of The Major Challenges İn İnternational Law İs The Lack Of Enforcement Of Binding Decisions.

Accordingly, The Proposed Model İntroduces A Distinct İnstitutional Layer Dedicated To **Monitoring And Ensuring The Execution Of Decisions**.

This İncludes:

- National Enforcement Units Within AI Courts;
- İnternational Enforcement Units Within The International AI Court Under The UN.

Core Functions İnclude:

- Monitoring The İmplementation Of Judicial Decisions;
- Ensuring The Effective Execution Of Sanctions;
- Proposing Additional Measures İn Cases Of Continued Violations;
- Generating Compliance Pressure On States And Private Actors.

Through This Structure, AI Liability Evolves From A Purely Theoretical Framework İnto An **Effective And Enforceable Global Legal System**.

7. Conclusion And Evaluation

This Study Has Examined The Problem Of Personal Data Protection İn The Context Of Artificial İntelligence (AI) And İts Transformative İmpact On Legal Liability Regimes. The Analysis Demonstrates That AI İs Not Merely A Technical Tool; Rather, İt Constitutes A Data-Driven Decision-Making Architecture That Fundamentally Reshapes The Nature Of Legal Responsibility. In Particular, The Expansion Of Data Processing Capacities, The Emergence Of Algorithmic İnference Mechanisms, And The İncreasing Autonomy Of AI Systems Have Rendered Classical Liability Frameworks—Based On The İdentification Of A Perpetrator And The Establishment Of Causation—İnsufficient.

The Examination Of The Concept Of Personal Data Within The Legal Systems Of The European Union, The Council Of Europe, And The United Nations Reveals That This Concept İs Being İnterpreted İn An İncreasingly Broad And Dynamic Manner. However, Despite A Degree Of Conceptual Convergence, Regulatory Frameworks Remain Fragmented İn Terms Of Binding Force, Scope, And İmplementation. The Proliferation Of Big Data Analytics, Pervasive Surveillance, And Cross-Border Data Flows Generates Significant Risks For İndividual Rights, Particularly İn Sensitive Sectors Such As Healthcare, Finance, And Public Administration. In This Context, Personal Data Can No Longer Be Understood As A Static Legal Category; Rather, İt Must Be Conceptualized As A Dynamic And Relational Construct Within The AI Ecosystem.

Building Upon This Theoretical Foundation, The Study Demonstrates That The Relationship Between AI Systems And Liability Law İs Evolving From An Act-Based Paradigm Toward A Data-Driven Structure. Harm Caused By AI Systems Rarely Results From A Single İdentifiable Act; İnstead, İt Emerges From Complex İnteractions Among Datasets, Algorithms, And Multiple Actors. This Transformation Gives Rise To New Legal Categories, İncluding İnference-Based Harm And Distributed Liability. Consequently, Traditional Models—Such As Fault-Based Liability, Strict Liability, And Product Liability—Are No Longer Sufficient When Applied İn İsolation.

The Comparative Analysis Of The European Union, The Council Of Europe, The United States, And China Clearly İndicates That A Unified Global Model Of AI Liability Has Not Yet Emerged. While The EU's Normative Strength And Rights-Based Approach, The Council Of Europe's Human Rights–Oriented Judicial Oversight, The U.S. Model's Flexibility And Market-Driven Structure, And China's State-Centered Control Paradigm Each Offer Distinct Advantages, None Provides A Comprehensive And Harmonized Global Liability Framework. This Fragmentation Underscores That AI Liability İs Not Solely A Legal İssue, But Also A Domain Shaped By Political, Economic, And İdeological Factors.

In Response To These Structural Limitations, This Study Proposes The **Layered Global Artificial Intelligence Liability System (G-AILS)** As A Novel Contribution To The Literature. The Proposed Model Consists Of:

(İ) A Normative Layer Establishing Global Foundational Principles;

(İi) A Liability Allocation Layer Based On A Risk-Oriented And Multi-Actor Framework;

(İii) An Enforcement And Adjudication Layer İncorporating National And İnternational AI Courts; And
(İv) A Compliance And Execution Layer Ensuring The Effective İmplementation Of Decisions.

The Most Significant İnnovation Of This Model Lies İn İts Extension Of Liability Beyond İndividual Actors To İnclude States And Global Governance Structures, Thereby Transforming Liability Law İnto A Systemic Framework.

Accordingly, The Central Thesis Of This Study May Be Formulated As Follows:

In The Age Of Artificial İntelligence, Legal Liability Must Evolve Beyond İndividual And National Boundaries İnto A Global And Systemic Structure.

Absent Such A Transformation, Legal Systems Will Continue To Lag Behind Technological Developments, Thereby Undermining Both The Protection Of İndividual Rights And Legal Certainty.

In Conclusion, This Study Reconceptualizes AI Liability As A Data-Centered, Multi-Actor, And Transnational Legal Paradigm, And Calls For A Transition From Reactive Regulation To Proactive Governance. In This Respect, İt Not Only İdentifies Existing Challenges But Also Offers A Theoretical And Normative Framework Capable Of Guiding Future Legal Developments İn The Field.

REFERENCES

Aletras, Nikolaos, Dimitrios Tsarapatsanis, Daniel Preoţiuc-Pietro, And Vasileios Lampos. 2016. “Predicting Judicial Decisions Of The European Court Of Human Rights: A Natural Language Processing Perspective.” *Peerj Computer Science* 2: E93. Https://Doi.Org/10.7717/Peerj-Cs.93.

Ashley, Kevin D. 2017. *Artificial Intelligence And Legal Analytics: New Tools For Law Practice İn The Digital Age*. Cambridge: Cambridge University Press.

Barocas, Solon, And Andrew D. Selbst. 2016. "Big Data's Disparate Impact." *California Law Review* 104(3): 671–732.

Calabresi, Guido. 1970. *The Costs Of Accidents: A Legal And Economic Analysis*. New Haven: Yale University Press.

Calo, Ryan. 2015. "Robotics And The Lessons Of Cyberlaw." *California Law Review* 103(3): 513–563.

Citron, Danielle Keats. 2008. "Technological Due Process." *Washington University Law Review* 85: 1249–1313.

Erkan, Fikret. 2023. "Scope And Legal Binding Of The European Court Of Human Rights Decisions." *Journal Of Economics And Social Research* 20: 24–31.

Erkan, Fikret. 2025. "Artificial Intelligence And Liability For Damages." *International Journal Of Social Sciences* 9(12): 297–343.

Erkan, Fikret. 2026. "Reconfiguring Judicial Legitimacy: Artificial Intelligence, Cognitive Bias, And The Rise Of Algorithmic Authority." *International Journal Of Social Sciences* 10(42): 159–220.

Gartner IT Glossary, "What Is Big Data?" 2018. [Online]. Available: Https://Www.Gartner.Com/İt-Glossary/Big-Data

Hacker, Philipp. 2022. "The European AI Liability Directives: Critique Of A Half-Hearted Approach And Lessons For The Future."

Hildebrandt, Mireille. "Law As Computation İn The Era Of Artificial Legal Intelligence." *Osgoode Hall Law Journal* 57, No. 1 (2020): 101–128.

Hillman, Noel L. "The Use Of Artificial Intelligence İn Gauging The Risk Of Recidivism." *The Judges' Journal* (2025).

Huchhanavar, Shivaraj S. "Conceptualising Judicial Independence And Accountability From A Regulatory Perspective." *Oslo Law Review* 9, No. 2 (2023): 110–148.

Hubbard, F. Patrick. 2014. "Sophisticated Robots: Balancing Liability, Regulation, And Innovation." *Florida Law Review* 66: 1803–1872.

IBM Think. (2024). Understanding The Types Of AI. Retrieved From Https://Www.İbm.Com/Think/Topics/Artificialintelligence-Types

Kahneman, Daniel. 2011. *Thinking, Fast And Slow*. New York: Farrar, Straus And Giroux.

Katz, Daniel Martin, Michael J. Bommarito II, And Josh Blackman. 2017. "A General Approach For Predicting The Behavior Of The Supreme Court Of The United States." *Plos ONE* 12(4): E0174698.

Keeton, W. Page, Dan B. Dobbs, Robert E. Keeton, And David G. Owen. 1984. *Prosser And Keeton On The Law Of Torts*. 5th Ed. St. Paul: West Publishing.

Kleinberg, Jon, Sendhil Mullainathan, And Manish Raghavan. 2017. "Inherent Trade-Offs İn The Fair Determination Of Risk Scores." *Proceedings Of ITCS*.

Lyon, David. *Surveillance Studies: An Overview*. Polity Press 2007.

Lohmann, Melinda F. 2016. "Liability Issues Concerning Self-Driving Vehicles." *European Journal Of Risk Regulation* 7(2): 335–340. Https://Doi.Org/10.1017/S1867299X00005754

Lumenalta. (2024). What Are The Different Types Of AI? Retrieved From Https://Lumenalta.Com/İnsights/What-Are-Thedifferent-Types-Of-Ai

Olabiyi, W., Akinyele, D., & Joel, E. (2025). The Evolution Of AI: From Rule-Based Systems To
Data-Driven İntelligence. "Journal Of Artificial Intelligence Evolution", 1(1), 1-20. Retrieved From
Https://Www.Researchgate.Net/Publication/388035967

Mostert, Menno, Annelien Bredenoord, Martijn Biesaart, And Johannes J. Delden. 2016. "Big Data İn Medical Research And EU Data Protection Law." *European Journal Of Human Genetics* 24(7): 956–960.

Narayanan, S., And M. Potkewitz. 2023. "A Risk-Based Approach To Assessing Liability Risk For AI-Driven Harms."

O'Neil, Cathy. 2016. *Weapons Of Math Destruction*. New York: Crown Publishing.

Oswald, Marion. 2022. "A Three-Pillared Approach To AI İn Policing." *European Journal Of Law And Technology* 13(1).

Pagallo, Ugo. 2013. *The Laws Of Robots: Crimes, Contracts, And Torts*. Dordrecht: Springer.

Pasquale, Frank. 2015. *The Black Box Society*. Cambridge, MA: Harvard University Press.

Russell, Stuart J., And Peter Norvig. 2010. *Artificial Intelligence: A Modern Approach*. 3rd Ed.

Simplilearn. (2025). Types Of Artificial Intelligence Explained. Retrieved From Https://Www.Simplilearn.Com/Tutorials/Artificial-İntelligence-Tutorial/Types-Of-Artificialintelligence

Surden, Harry. 2014. "Machine Learning And Law." *Washington Law Review* 89(1): 87–115.

Selbst, Andrew D., Et Al. "Fairness And Abstraction İn Sociotechnical Systems." *Proceedings Of FAT* (2019).

Sharma, M. "India's Courts And Artificial Intelligence: A Future Outlook." *Lexonomica* 15, No. 1 (2023): 99–120.

Shoshana Zuboff, *The Age Of Surveillance Capitalism* (Publicaffairs 2019).

Solon Barocas And Andrew D. Selbst, "Big Data's Disparate Impact," *California Law Review* 104, No. 3 (2016): 671–732.

Sunstein, Cass R., Et Al. *Punitive Damages: How Juries Decide.* Chicago: University Of Chicago Press, 2002.

Surden, Harry. "Machine Learning And Law." *Washington Law Review* 89, No. 1 (2014): 87–115.

Tegmark, Max. 2017. *Life 3.0: Being Human İn The Age Of Artificial Intelligence*. New York: Knopf.

UN Human Rights Council. 2021. *The Right To Privacy İn The Digital Age*. UN Doc A/HRC/48/31.

Wachter, Sandra, Brent Mittelstadt, And Luciano Floridi. 2017. "Why A Right To Explanation Does Not Exist İn GDPR." *International Data Privacy Law* 7(2): 76–99.

Zuboff, Shoshana. 2019. *The Age Of Surveillance Capitalism*. New York: Publicaffairs.

Xu, B. (2024, April 16). What İs Meant By AGI? On The Definition Of Artificial General İntelligence
[Preprint]. Arxiv. Https://Doi.Org/10.48550/Arxiv.2404.10731